ESET

REMOTE ADMINISTRATOR 6

Installation Manual and User Guide

Click here to navigate to the most recent version of this document

ENJOY SAFER TECHNOLOGY™

ESET **REMOTE ADMINISTRATOR 6**

Copyright © 2015 by ESET, spol. s r.o.
ESET Remote Administrator 6 was developed by ESET, spol. s r.o.

For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care: www.eset.com/support

REV. 28/04/2015

Contents

1. Introduction 6

1.1 Features 6

1.2 Architecture 7

1.2.1 Server 8

1.2.2 Web Console 9

1.2.3 Agent 9

1.2.4 Proxy 10

1.2.5 Rogue Detection Sensor 11

1.2.6 Mobile Device Connector 12

1.2.7 Deployment scenarios 13

1.2.7.1 Single Server (Small Business) 13

1.2.7.2 Remote Branches with Proxies 14

1.2.7.3 High Availability (Enterprise) 15

1.2.8 Practical deployment examples 16

1.3 Supported products and languages 17

2. System requirements 19

2.1 Hardware 19

2.2 Database 19

2.3 Supported Operating Systems 20

2.3.1 Windows 20

2.3.2 Linux 22

2.3.3 OS X 22

2.4 Ports used 23

3. Installation process 25

3.1 Package installation 25

3.1.1 Installation on Windows SBS / Essentials 27

3.2 Database 30

3.2.1 Database Server Backup 30

3.2.2 Database Server Upgrade 30

3.2.3 ERA Database Migration 31

3.2.3.1 Migration process for SQL Server 31

3.2.3.2 Migration process for MySQL Server 39

3.3 ISO image 40

3.4 Virtual appliance 41

3.4.1 VMware Player 44

3.4.2 Oracle VirtualBox 45

3.4.3 Microsoft Hyper-V 45

3.5 Failover Cluster - Windows 46

3.6 Failover Cluster - Linux 47

3.7 Component installation on Windows 49

3.7.1 Server installation - Windows 49

3.7.1.1 Server prerequisites - Windows 51

3.7.2 Microsoft SQL Server - Windows 52

3.7.3 Agent installation - Windows 52

3.7.4 Web Console installation - Windows 53

3.7.4.1 Supported Web browsers 53

3.7.5 Proxy installation - Windows 54

3.7.5.1 Proxy prerequisites - Windows 54

3.7.6 RD Sensor installation - Windows 55

3.7.6.1 RD Sensor prerequisites - Windows 55

3.7.7 Mobile Device Connector installation - Windows 55

3.7.7.1 Mobile Device Connector prerequisites - Windows 58

3.7.8 Apache HTTP Proxy installation - Windows 59

3.8 Component installation on Linux 60

3.8.1 Server installation - Linux 60

3.8.1.1 Server prerequisites - Linux 62

3.8.2 Agent installation - Linux 63

3.8.2.1 Agent prerequisites - Linux 64

3.8.3 ERA Web Console installation - Linux 64

3.8.3.1 ERA Web Console prerequisites - Linux 64

3.8.4 Proxy installation - Linux 65

3.8.4.1 Proxy prerequisites - Linux 66

3.8.5 RD Sensor installation and prerequisites - Linux 66

3.8.6 Mobile Device Connector installation - Linux 66

3.8.6.1 Mobile Device Connector prerequisites - Linux 68

3.8.7 Apache HTTP Proxy installation - Linux 68

3.8.7.1 Squid 70

3.8.8 How to uninstall or reinstall a component - Linux 71

3.9 DNS Service Record 72

3.10 Migration Tool 73

3.10.1 Migration scenario 1 74

3.10.2 Migration scenario 2 76

3.10.3 Migration scenario 3 79

4. First Steps 82

4.1 Opening the ERA Web Console 82

4.2 The ERA Web Console login screen 84

4.3 Getting to know ERA Web Console 85

4.4 Deployment 87

4.4.1 Add client computer to ERA structure 88

4.4.1.1 Using Active Directory synchronization 88

4.4.1.2 Manually typing name/IP 89

4.4.1.3 Using RD Sensor 91

4.4.2 Agent deployment 93

4.4.2.1 Deployment steps - Windows 94

4.4.2.1.1 Agent Live Installers 95

4.4.2.1.2 Deploy Agent remotely 98

4.4.2.1.3 Deploy Agent locally 103

4.4.2.2 Deployment steps - Linux 106

4.4.2.3 Deployment steps - OS X 106

4.4.2.4 Troubleshooting - Agent deployment 107

4.4.3 Agent deployment using GPO and SCCM 108

4.4.3.1 Creating MST file 109

4.4.3.2 Deployment steps - GPO 115

4.4.3.3 Deployment steps - SCCM 119

4.4.4 Product installation 135

4.4.4.1 Product installation (command line) 137

4.4.4.2 List of problems when installation fails 138

4.5 Management 139

4.5.1 Add computers to groups 139
4.5.1.1 Static groups 139
4.5.1.1.1 Add computer to a static group 140
4.5.1.2 Dynamic groups 141
4.5.1.2.1 New Dynamic Group Template 142
4.5.1.2.2 Create new Dynamic Group 143
4.5.2 Create a new policy 146
4.5.3 Assign a policy to a group 149
4.5.4 Mobile Device enrollment 151

4.6 Best practices 152
4.6.1 User Management 152

5. Working with ESET Remote Administrator 153

5.1 Dashboard 153
5.1.1 Dashboard settings 154
5.1.2 Drill down 156
5.1.3 Edit report template 157

5.2 Computers 161
5.2.1 Add Computers 163
5.2.2 Computer details 165

5.3 Threats 166

5.4 Reports 167
5.4.1 Create a new report template 168
5.4.2 Generate report 171
5.4.3 Schedule a report 171
5.4.4 Outdated applications 171

6. Administration of ESET Remote Administrator 172

6.1 Admin 172
6.1.1 Groups 172
6.1.1.1 Create new Static Group 174
6.1.1.2 Create new Dynamic Group 177
6.1.1.3 Assign Task to a Group 180
6.1.1.4 Assign a Policy to a Group 182
6.1.1.5 Policies and Groups 183
6.1.1.6 Static Groups 183
6.1.1.6.1 Static Group Wizard 184
6.1.1.6.2 Manage Static Groups 185
6.1.1.6.3 Move Static Group 186
6.1.1.6.4 Add Client Computer to Static Group 187
6.1.1.6.5 Import clients from Active Directory 189
6.1.1.6.6 Assign a Task to a Static Group 189
6.1.1.6.7 Assign a Policy to a Static Group 189
6.1.1.6.8 Export Static Groups 190
6.1.1.6.9 Import Static Groups 191
6.1.1.7 Dynamic Groups 192
6.1.1.7.1 Dynamic Group Template Wizard 192
6.1.1.7.2 Manage Dynamic Group Templates 193
6.1.1.7.3 Dynamic Group Wizard 195
6.1.1.7.4 Create Dynamic Group using existing Template 196
6.1.1.7.5 Create Dynamic Group using new Template 199
6.1.1.7.6 Manage Dynamic Groups 199
6.1.1.7.7 Move Dynamic Group 201
6.1.1.7.8 Assign a Policy to a Dynamic Group 202
6.1.1.7.9 Assign a Task to a Dynamic Group 202
6.1.1.7.10 How to automate ESET Remote Administrator 202
6.1.1.7.11 When does a computer become a member of a Dynamic Group? 203
6.1.1.7.12 Template Rules Evaluation 203
6.1.1.7.13 Rule Editor 205
6.1.2 Policies 206
6.1.2.1 Policies Wizard 207
6.1.2.2 Flags 208
6.1.2.3 Manage Policies 209
6.1.2.4 How Policies are applied to clients 212
6.1.2.4.1 Ordering Groups 212
6.1.2.4.2 Enumerating Policies 213
6.1.2.4.3 Merging Policies 214
6.1.2.5 Configuration a product from ERA 214
6.1.2.6 Assign Policy to Group 215
6.1.2.7 Assign a Policy to a Client 217
6.1.3 Client Tasks 218
6.1.3.1 Client Task Wizard 220
6.1.3.2 Manage Client Tasks 223
6.1.3.2.1 On-Demand Scan 224
6.1.3.2.2 Operating System Update 226
6.1.3.2.3 Quarantine Management 227
6.1.3.2.4 Rogue Detection Sensor Database Reset 228
6.1.3.2.5 Remote Administrator Components Upgrade 229
6.1.3.2.6 Reset Cloned Agent 231
6.1.3.2.7 Run Command 232
6.1.3.2.8 Run SysInspector Script 233
6.1.3.2.9 Software Install 234
6.1.3.2.10 Software Uninstall 236
6.1.3.2.11 Product Activation 237
6.1.3.2.12 SysInspector Log Request 239
6.1.3.2.13 Upload Quarantined File 240
6.1.3.2.14 Virus Signature Database Update 241
6.1.3.2.15 Virus Signature Database Update Rollback 243
6.1.3.2.16 Display Message 244
6.1.3.2.17 Anti-Theft Action 245
6.1.3.2.18 Device Enrollment 247
6.1.3.2.19 Stop Managing (Uninstall ERA Agent) 260
6.1.3.3 Export Managed Products Configuration 262
6.1.3.4 Assign Task to Group 263
6.1.3.5 Assign Task to Computer(s) 265
6.1.3.6 Schedule a Task 267
6.1.3.7 Triggers 268
6.1.4 Server Tasks 268
6.1.4.1 Server Task Wizard 268
6.1.4.2 Manage Server Tasks 269
6.1.4.2.1 Agent Deployment 269
6.1.4.2.2 Generate Report 274

Contents

6.1.4.2.3 Static Group Synchronization 277
6.1.4.2.4 Static Group Synchronization - Linux Computers 278
6.1.4.3 Scheduling Server Task 279
6.1.4.4 Reuse Trigger in Server Task 279
6.1.4.5 Triggers 280
6.1.4.5.1 Throttling 281
6.1.4.5.1.1 Trigger is too sensitive 283
6.1.4.5.2 Server Trigger Wizard 284
6.1.4.5.3 Manage Server Triggers 285
6.1.4.5.3.1 Trigger fires too often 286
6.1.4.5.3.2 CRON Expression 287
6.1.4.5.4 Manage Trigger Sensitivity 287
6.1.5 Notifications 289
6.1.5.1 Notifications Wizard 290
6.1.5.2 Manage Notifications 293
6.1.5.3 How to configure an SNMP Trap Service 295
6.1.6 Certificates 296
6.1.6.1 Peer Certificates 297
6.1.6.1.1 Create a new Certificate using the ERA Certification Authority 298
6.1.6.1.2 Create a new Certificate using a custom Certificate Authority 299
6.1.6.2 Certificate Authorities 299
6.1.6.2.1 Create a new Certificate Authority 300
6.1.7 Access Rights 301
6.1.7.1 Users 301
6.1.7.1.1 Mapped Domain Security Group Wizard 302
6.1.7.1.2 Native User Wizard 303
6.1.7.1.3 Create a Native User 304
6.1.7.1.3.1 Create New Admin account 305
6.1.7.1.4 Map Group to Domain Security Group 305
6.1.7.1.5 Assign User a Permission Set 306
6.1.7.2 Permission Sets 307
6.1.7.2.1 Permission Set Wizard 309
6.1.7.2.2 Manage Permission Sets 310
6.1.8 Server Settings 311
6.1.9 License Management 312
6.1.9.1 Activation 314

7. Diagnostic Tool 319

8. Glossary 320

8.1 Types of infiltration 320
8.1.1 Viruses 320
8.1.2 Worms 320
8.1.3 Trojan horses 321
8.1.4 Rootkits 321
8.1.5 Adware 321
8.1.6 Spyware 322
8.1.7 Potentially unsafe applications 322
8.1.8 Potentially unwanted applications 322

9. FAQ 323

10. About ESET Remote Administrator 325

11. End-User License Agreement (EULA) 326

1. Introduction

ESET Remote Administrator (ERA) is an application that allows you to manage ESET products on client workstations, servers and mobile devices in a networked environment from one central location. With ESET Remote Administrator's built-in task management system, you can install ESET security solutions on remote computers and quickly respond to new problems and threats.

ESET Remote Administrator on its own does not provide protection against malicious code. Protection of your environment depends on the presence of an ESET security solution such as ESET Endpoint Security or ESET File Security for Microsoft Windows Server on workstations, servers or mobile devices.

ESET Remote Administrator 6 is built around two primary principles:

1. **Centralized management** - the entire network can be configured, managed and monitored from one place.
2. **Scalability** - the system can be deployed in a small network as well as in large enterprise environments. Extension/scaling of the system is designed to easily accommodate the growth of your infrastructure.

The ESET Remote Administrator help pages offer you a complete user administration guide. We recommend that you begin by becoming familiar with frequently used parts of ESET Remote Administrator:

- Architecture of ESET Remote Administrator
- Installation processes and Deployment processes
- Agent deployment using GPO or SCCM
- First steps after installing ESET Remote Administrator
- Getting to know ERA Web Console
- Working with ESET Remote Administrator
- Administration
- Migration Tool

1.1 Features

The following features and capabilities are new in version 6:

- Platform independency - ERA Server works on both Windows and Linux!
- ERA Web Console, the primary user interface for ESET Remote Administrator, is accessed using your web browser. This makes it easy to use from any place and any device.
- A fully customizable Dashboard gives you a great overview of the security state of your network and the Admin section of ESET Remote Administrator Web Console (ERA Web Console) is a powerful and user-friendly tool for managing ESET products.
- Notifications deliver relevant information in real time and Reports allows you to conveniently sort various types of data that you can use later.

1.2 Architecture

To perform a complete deployment of the ESET security solutions portfolio, the following components must be installed (Windows platform):

- ERA Server
- ERA Database
- ERA Web Console
- ERA Agent

To perform a complete deployment of the ESET security solutions portfolio, the following components must be installed (Linux platform):

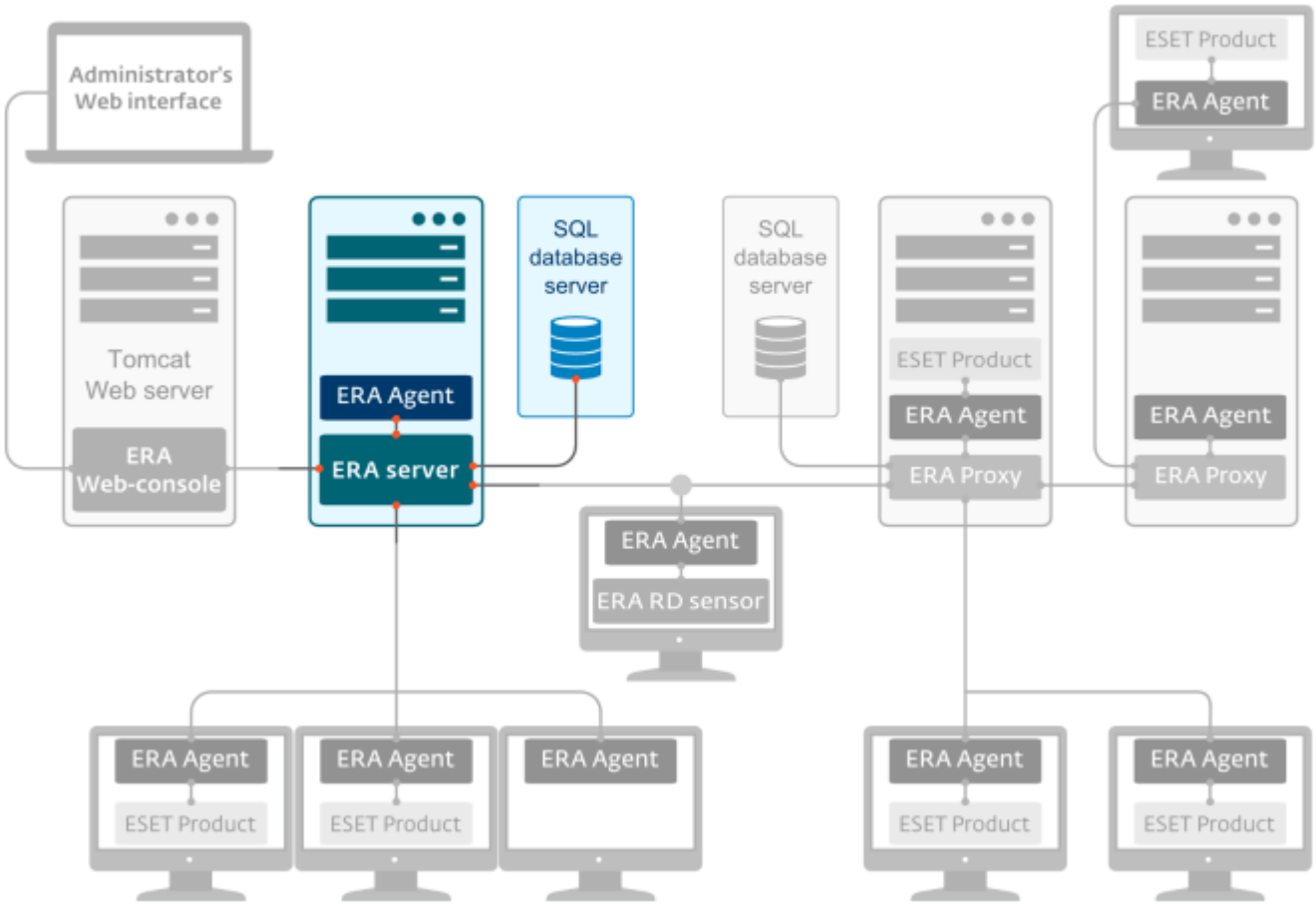
- ERA Server
- ERA Web Console
- ERA Agent

The following supporting components are optional, we recommend that you install them for best performance of the application on the network:

- ERA Proxy
- RD Sensor
- Mobile Device Connector
- Apache HTTP Proxy

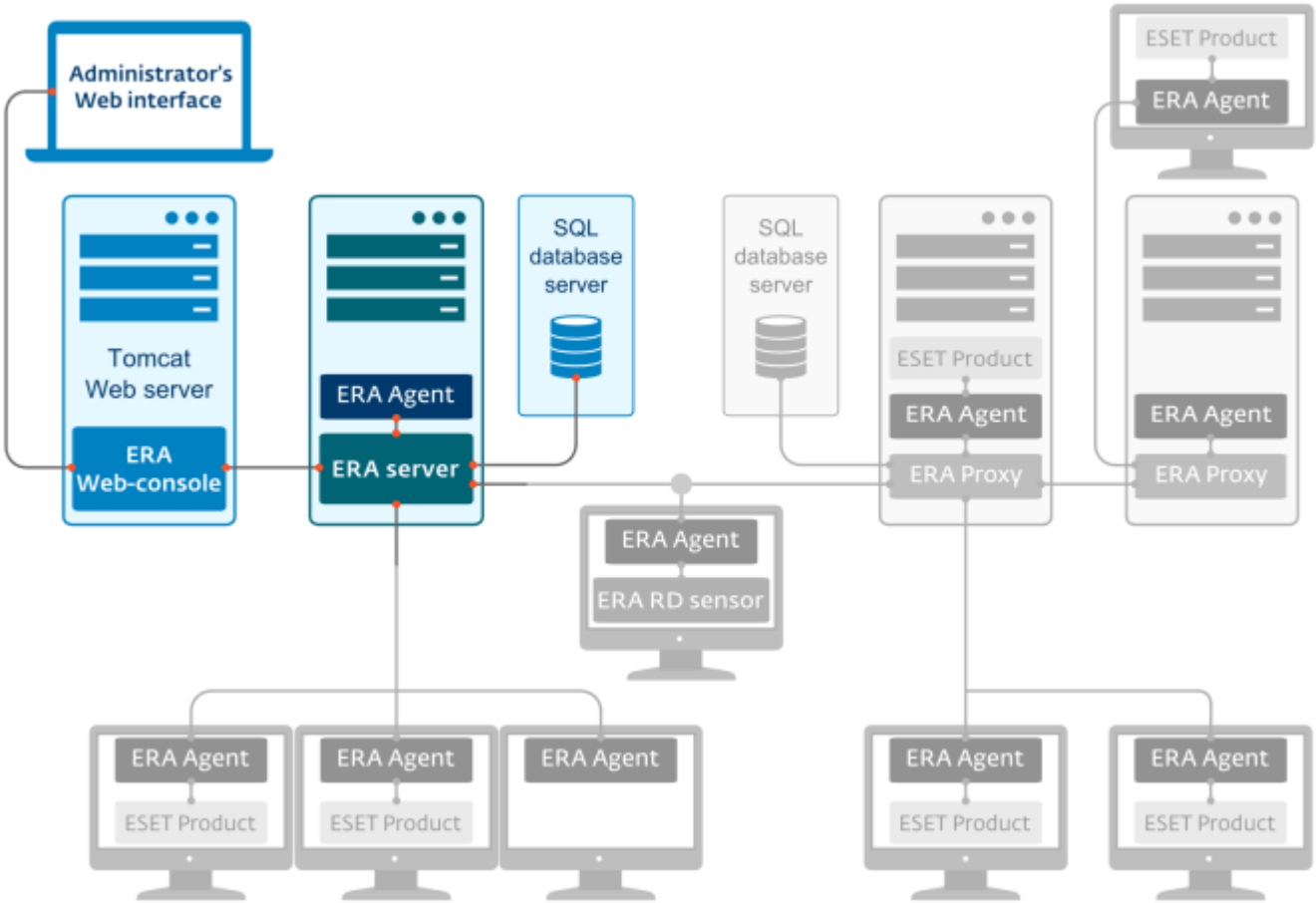
1.2.1 Server

ESET Remote Administrator Server is the executive application that processes all data received from clients that connect to the Server (through the ERA Agent). To correctly process data, the Server requires a stable connection to a database server where network data is stored. We recommend that you install the database server on a different computer to achieve better performance.



1.2.2 Web Console

ERA Web Console is a web-based user interface that allows you to manage ESET security solutions in your environment. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. The Web Console is accessed using your browser (see Supported Web browsers). If you choose to make the web server accessible from the internet, you can use ESET Remote Administrator from virtually any place and device.



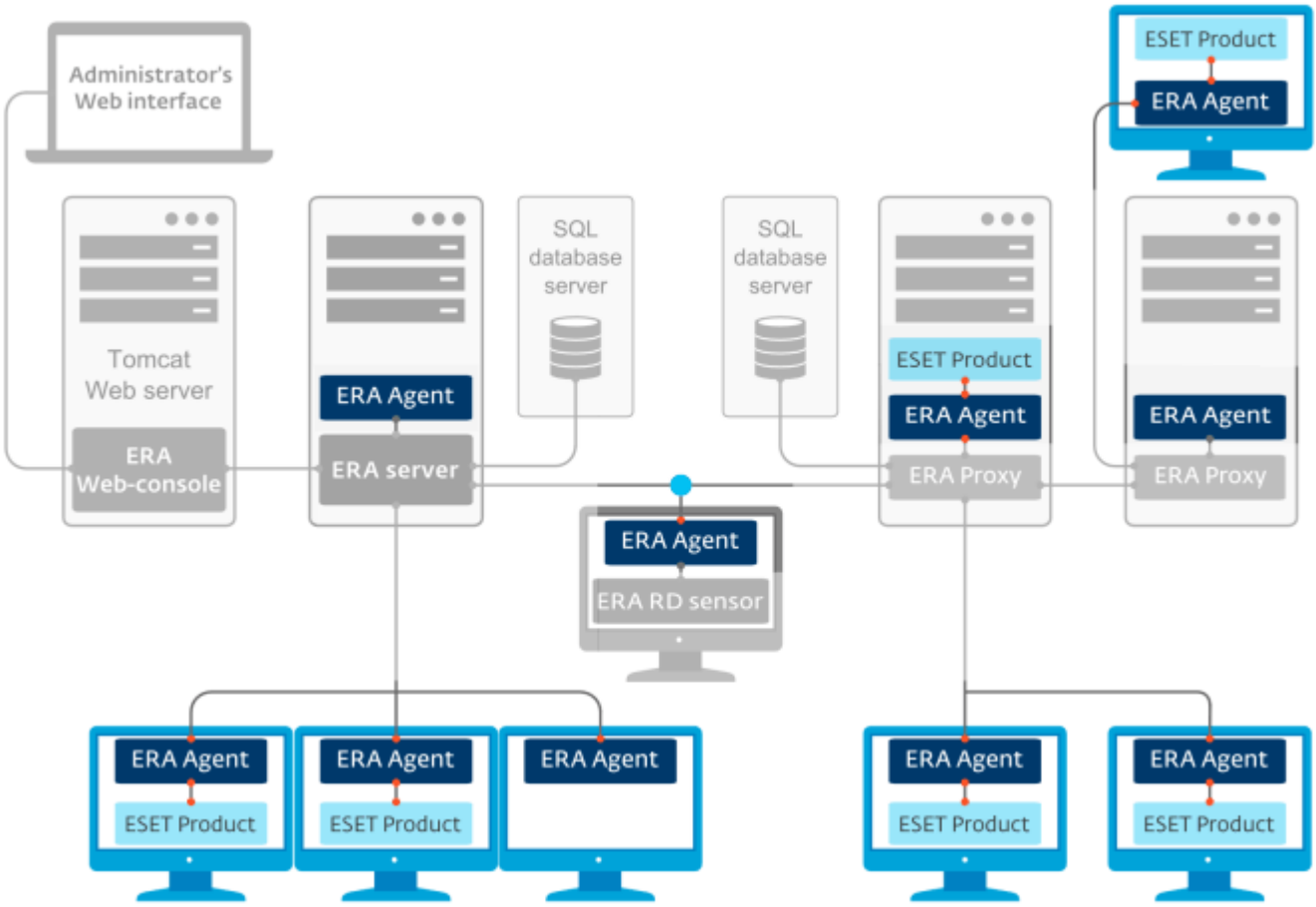
1.2.3 Agent

The Agent is an essential part of ESET Remote Administrator. Clients do not communicate with the Server directly, rather the Agent facilitates this communication. The Agent collects information from the client and sends it to the ERA Server. If the ERA Server sends a task for the client - it is sent to the Agent which then sends this task to the client.

To simplify implementation of the endpoint protection the stand-alone ERA Agent is included in the ERA suite (from version 6). It is simple, highly modular and lightweight service covering all communication between ERA Server and any ESET product or operating system. Rather than communicate with the ERA Server directly, ESET products communicate through the Agent. Client computers that have ESET Agent installed and can communicate with the ERA Server are referred to as 'managed'. You can install the Agent on any computer regardless of whether or not other ESET software has been installed.

The benefits are:

- Easy set-up – it is possible to deploy Agent as a part of standard corporate installation.
- On-place security management – since the Agent can be configured to store several security scenarios, reaction time to threat is significantly lowered.
- Off-line security management – the Agent can respond to an event if it is not connected to the ERA Server.



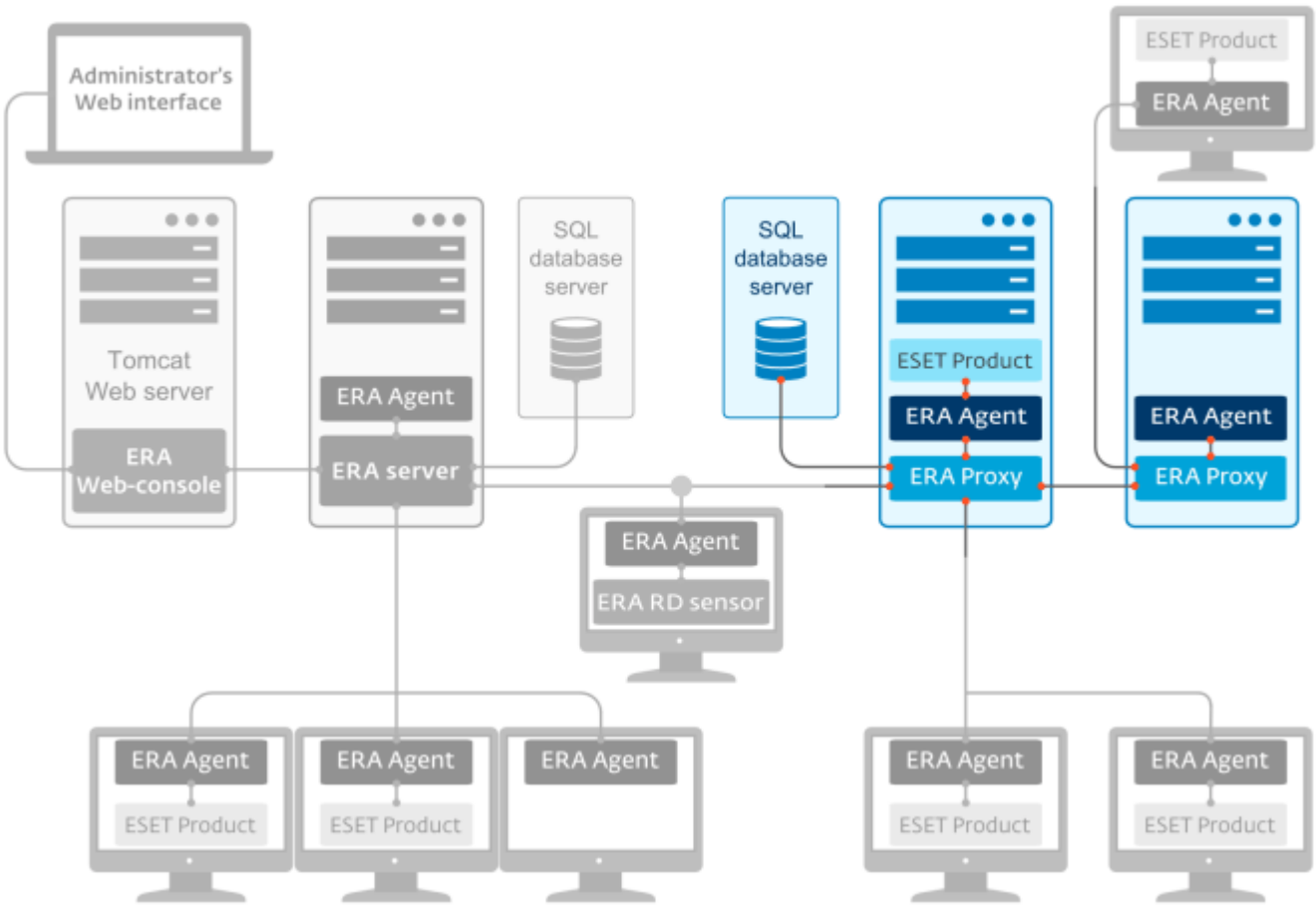
1.2.4 Proxy

ERA Proxy server is a lightweight version of the server component. This type of server is used to allow a high degree of scalability. The ERA Proxy server allows you to concentrate traffic from client Agents. It allows multiple Agents to connect to the ERA Proxy, which then distributes traffic to the ERA Server. This allows for the optimization of database queries. It is also possible for the ERA Proxy to connect to other Proxy servers and then to the ERA Server. Everything depends on the network environment and its configuration.

The ERA Proxy is also responsible for passive distribution of configuration data (groups, policies, tasks, etc.) to Agents. This forwarding is done with no involvement from the ERA Server.

The only way to configure the ERA Proxy (and all other components) is via policy sent from the ERA Server. This means that the Agent must be installed on the ERA Proxy machine to deliver the configuration from the ERA Server to the ERA Proxy component.

NOTE: It is not possible for the ERA Server to connect to the ERA Proxy server directly without the Agent.



ERA Proxy is another component of ESET Remote Administrator and serves two purposes. In the case of a medium-sized or enterprise network with many clients (for example, 10,000 clients or more), you can use ERA Proxy to distribute load between multiple ERA Proxies, thereby distributing load away from the main ERA Server. Another advantage of the ERA Proxy is that you can use it when connecting to a remote branch office with a weak link. This means that ERA Agent on each client is not connecting to the main ERA Server directly, but rather via ERA Proxy, which is on the same local network of the branch office. This configuration offers better communication with the branch office. The ERA Proxy accepts connections from all local ERA Agents, compiles their data and uploads it to the main ERA Server (or another ERA Proxy). This allows your network to accommodate more clients without compromising the performance of your network and database queries.

For proper function of the ERA Proxy, the host computer where you install ERA Proxy must have an ESET Agent installed and must be connected to the upper level (either ERA Server or an upper ERA Proxy, if there is one) of your network.

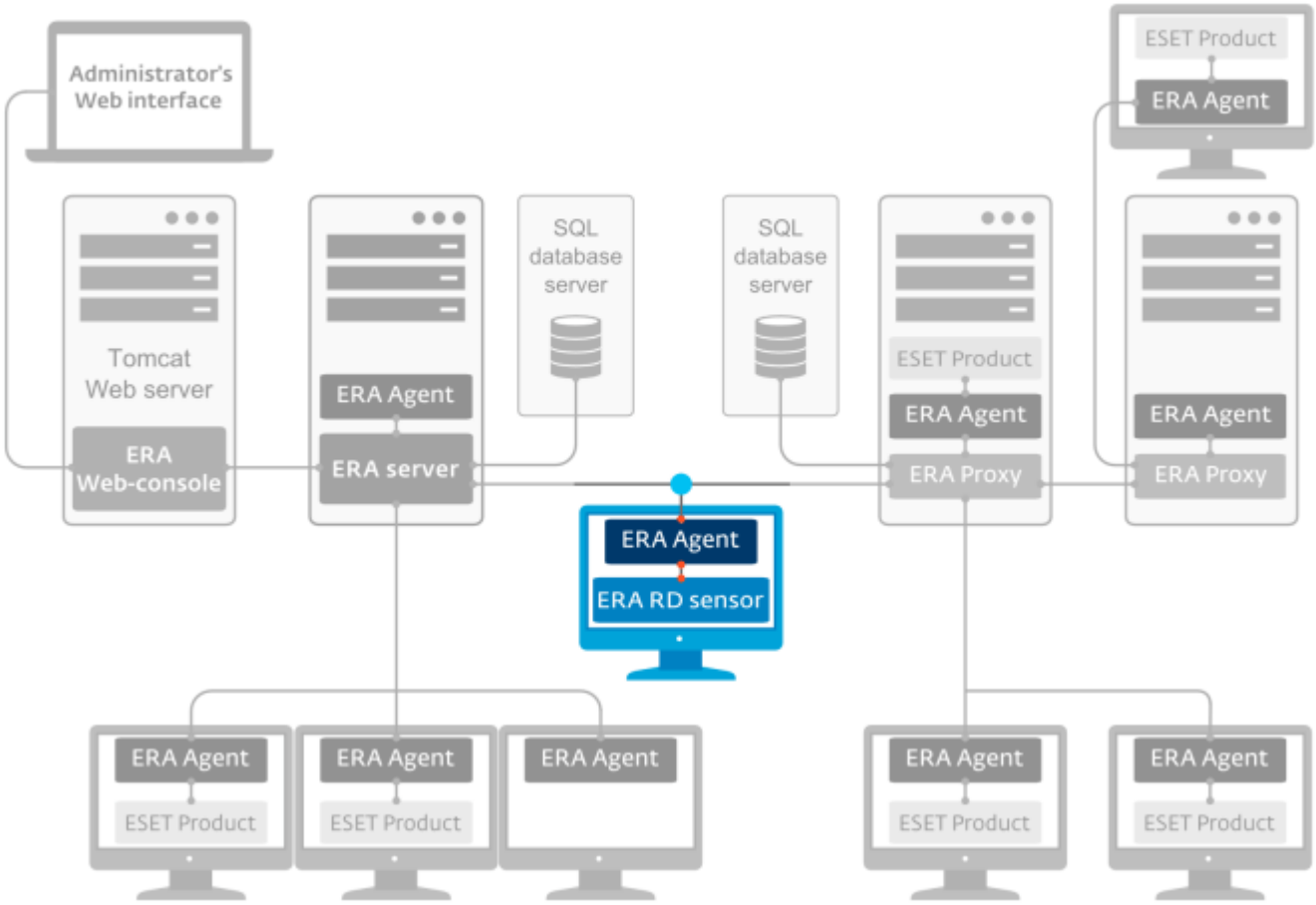
NOTE: See deployment scenario with ERA Proxy.

1.2.5 Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) is a rogue system detector tool that searches your network for computers. The Sensor is convenient because it can locate new computers from ESET Remote Administrator without the need to search and add them manually. Discovered machines are immediately located and reported in a predefined report, allowing you to move them to specific static groups and proceed with management tasks.

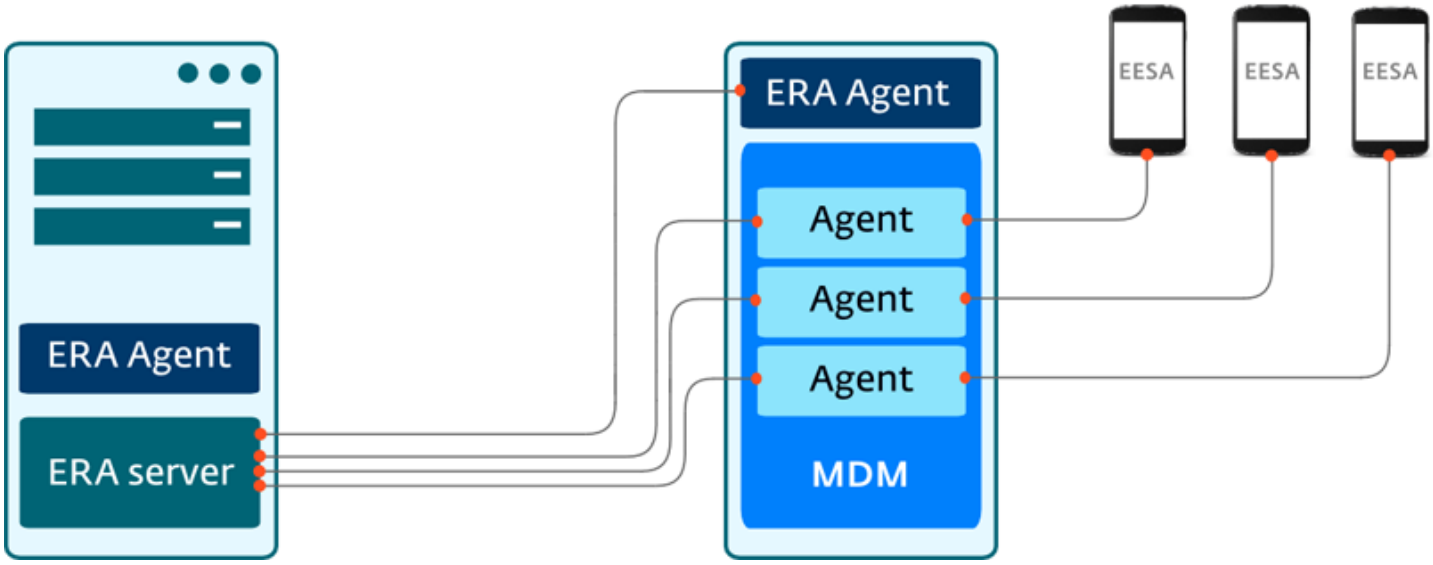
RD Sensor is a passive listener that detects computers that are present on the network and sends information about them to the ERA Server. ERA Server then evaluates whether the PCs found on the network are unknown to ERA Server or already managed.

Every computer within the network structure (domain, LDAP, Windows network) is added to ERA Server's computers list automatically via a server synchronization task. Using RD sensor is a convenient way to find computers that are not in the domain or other network structure and add them to ESET Remote Administrator Server. RD Sensor remembers computers that are already discovered and will not send the same information twice.



1.2.6 Mobile Device Connector

Mobile Device Connector is an application that lets you manage mobile devices and administer ESET Endpoint Security for Android.



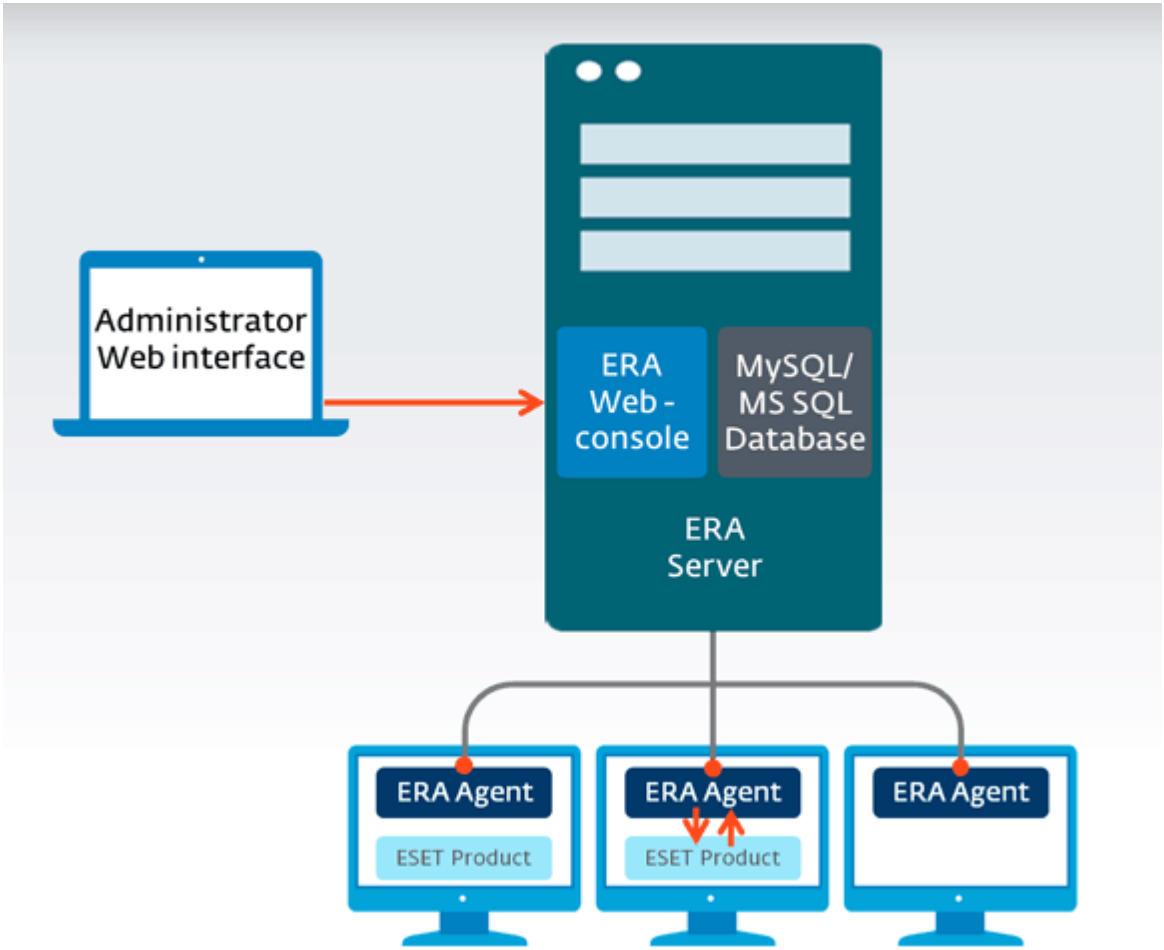
1.2.7 Deployment scenarios

In the following chapters, we will cover deployment scenarios for different network environments. For more detailed instructions, see the appropriate chapter:

- Single Server (Small Business)
- High Availability (Enterprise)
- Remote Branches with Proxies

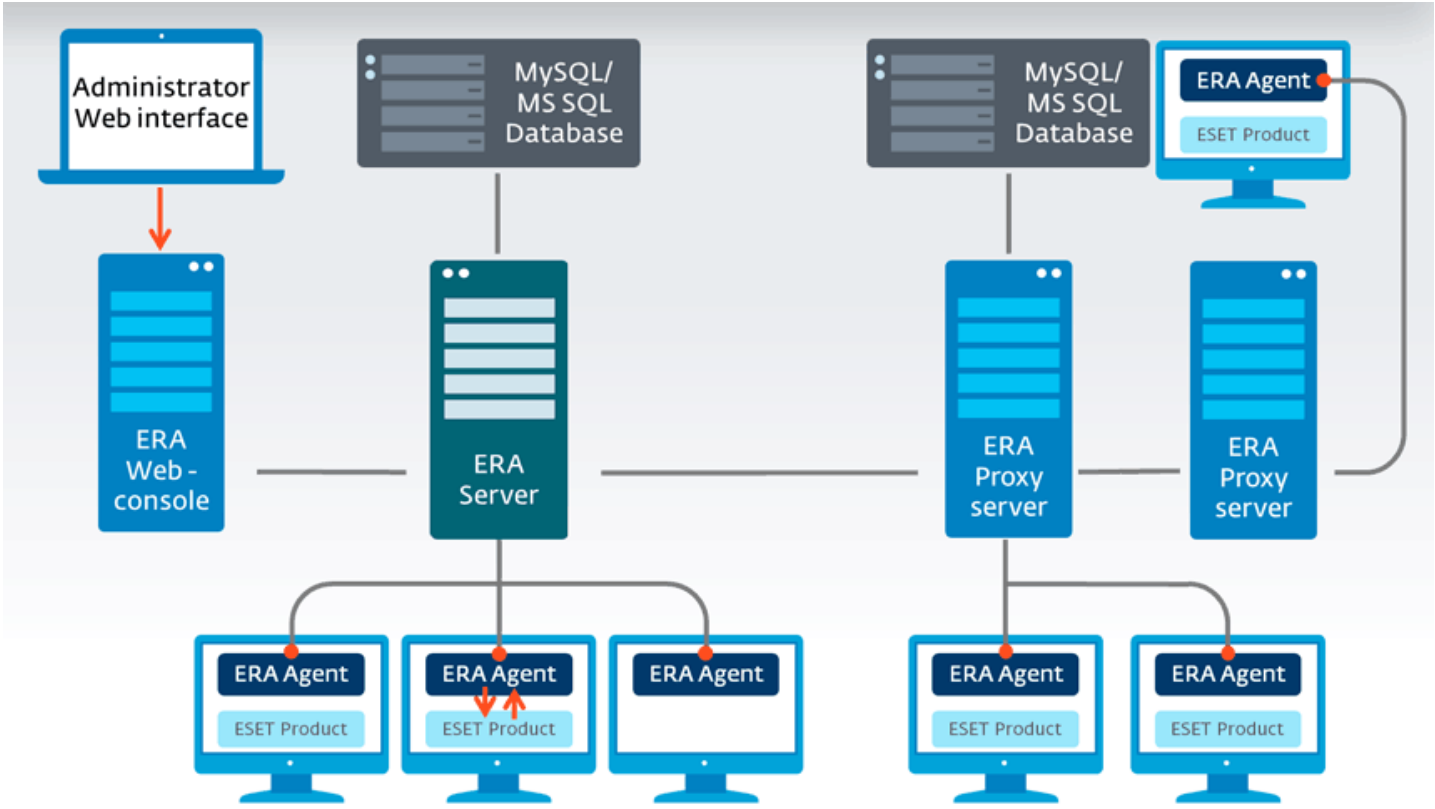
1.2.7.1 Single Server (Small Business)

To manage small networks (1000 clients or less), a single machine with ERA Server and all it's components (supplied web server, database, etc.) installed on it is usually sufficient. You can think of it as a single server or standalone installation. All managed clients are connected directly to the ERA Server via ERA Agent. The administrator can connect to the ERA Web Console via web browser from any computer on the network or run the Web Console directly from the ERA Server.



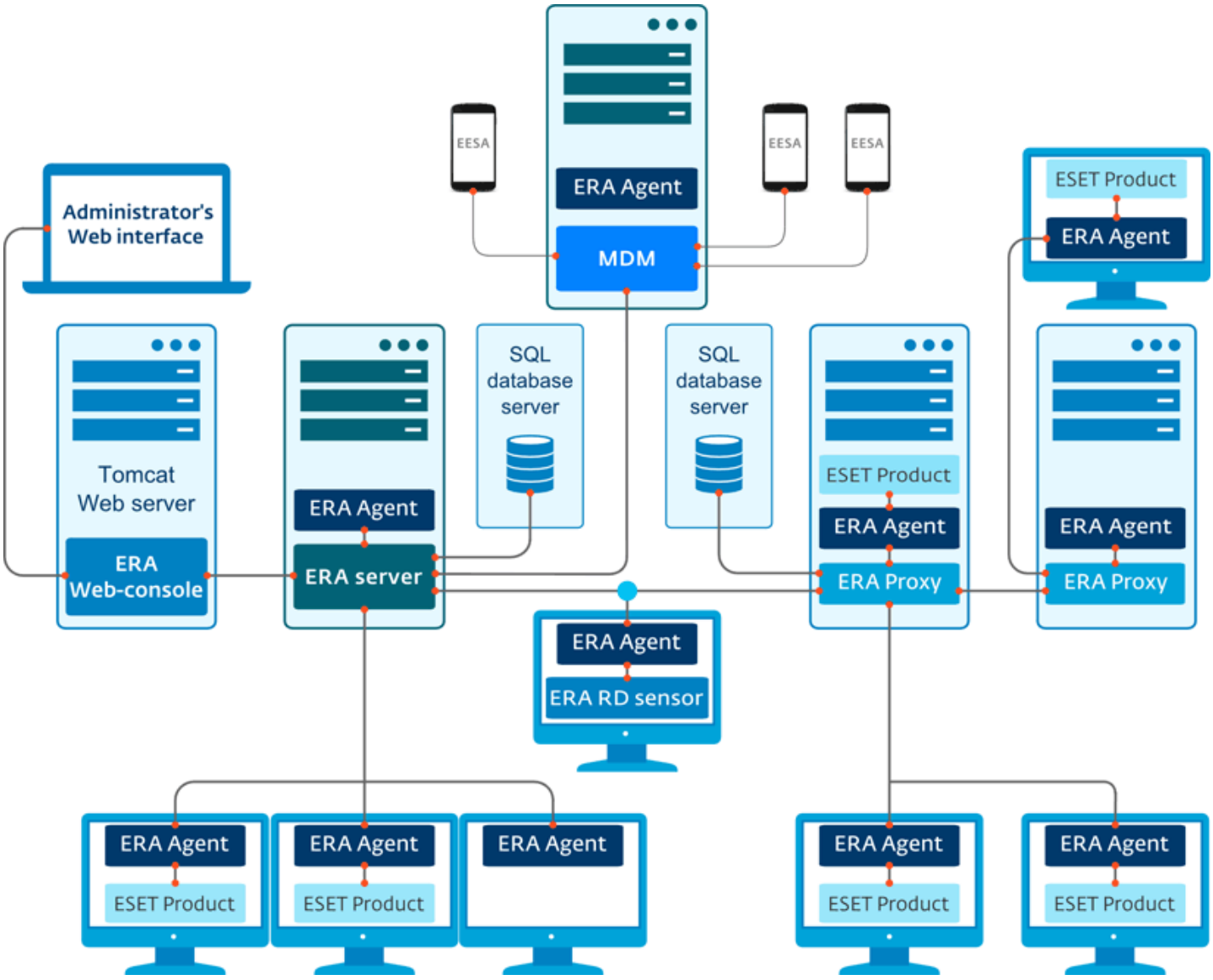
1.2.7.2 Remote Branches with Proxies

In a medium-sized network (for example, 10,000 clients), an additional layer which consists of ERA Proxy servers is added. ERA Agents are connected to the ERA Proxy server, the reason for the inclusion of the ERA Proxy server can be a weak link to the remote site (branch office). However, it is still possible to connect the ERA Agents (located on a remote site) directly to the main server.



1.2.7.3 High Availability (Enterprise)

For enterprise environments (for example, 100,000 clients), additional ERA components should be employed. One is RD Sensor, which helps to search your network and discover new computers. Another addition is a layer of ERA Proxy servers. ERA Agents are connected to the ERA Proxy server, thereby balancing the load on the master server which is important for performance. Using this configuration it is still possible to connect the ERA Agents directly to the main server. A SQL database is also implemented on a Failover Cluster to provide redundancy.



1.2.8 Practical deployment examples

For best performance, we recommend that you use Microsoft SQL Server as your ESET Remote Administrator database. While ESET Remote Administrator is compatible with MySQL, using MySQL can negatively impact system performance when working with large amounts of data including dashboards, threats and clients. The same hardware with Microsoft SQL Server is capable of handling about 10x the number of clients as with MySQL.

For testing purposes each client stores about 30 logs in the database. Microsoft SQL Server uses large quantities of RAM to cache database data, so we recommend that you have at least as much memory as Microsoft SQL Server has on disk.

There is no easy way to calculate the exact amount of resources used by ESET Remote Administrator since resources used will vary depending on your network configuration. Below are test results for common network configurations:

- Test case - maximum of 5,000 clients connecting to ERA Server
- Test case - maximum of 100,000 clients connecting to ERA Server

To achieve the optimum configuration for your needs, we recommend that you test with a smaller number of clients and slower hardware and project your system requirements based on test results.

TEST CASE (5,000 CLIENTS)

Hardware/software

- Windows Server 2003 R2, x86 processor architecture
- Microsoft SQL Server Express 2008 R2
- Intel Core2Duo E8400 @3 GHz
- 3 GB RAM
- Seagate Barracuda 7200rpm, 500GB, 16MB cache, Sata 3.0 Gb/s

Results

- ERA Web Console is very responsive (less than 5s)
- Memory consumption:
  - Apache Tomcat 200 MB
  - ERA Server 200 MB
  - SQL Server Database 1 GB
- Server replication performance 10 replications per second
- Database size on disk 1GB (5,000 clients, each with 30 logs in database)

For this example, SQL Server Express 2008 R2 was used. In spite of its limits (10GB database, 1CPU and 1GB of RAM usage), this configuration was functional and performed well. Using SQL Server Express is recommended for servers with less than 5,000 clients. You can deploy SQL Server Express initially and upgrade to Microsoft SQL Server (full version) when a larger database becomes necessary. Be aware that older Express versions (<2008 R2) have a database size limit of 4GB on disk.

Server replication performance defines a replication interval for clients. 10 replications per second results in 600 replications per minute. So in an ideal case, the replication interval on all 5000 clients should be set to 8 minutes, however this would incur a 100% load on the server, so a longer interval is necessary in this case. In this example, a 20-30 minute replication interval is recommended.

TEST CASE (100,000 CLIENTS)

Hardware/software

- Windows Server 2012 R2 Datacenter, x64 processor architecture
- Microsoft SQL Server 2012
- Intel Xeon E5-2650v2 @2.60GHz
- 64 GB RAM
- Network adapter Intel NIC/PRO/1000 PT Dual
- 2x Micron RealSSD C400 256GB SSD Drives (one for system+software, second for SQL Server Data Files)

Results

- Web Console is responsive (less than 30s)
- Memory consumption
  - Apache Tomcat 1 GB
  - ERA Server 2 GB
  - SQL Server Database 10 GB
- Server replication performance 80 replications per second
- Database size on disk 10 GB (100,000 clients, each with 30 logs in database)

In this case we chose to install all components (Apache Tomcat + Web Console, ERA Server, SQL Server) on one machine to test the capacity of the ERA Server.

The large number of clients resulted in increased memory and disk usage by Microsoft SQL Server. SQL Server chaches almost entirely from the database stored in memory for optimum performance. Apache Tomcat (Web Console) and ERA Server cache data as well, which explains the increased memory usage in this example.

ERA Server is capable of serving 80 replications per second (288,000 per hour), so in an ideal case, the replication interval on all 100,000 clients should be set to every ~30 minutes (load 200,000 replications per hour), but this will result in 100% server load, so the best replication interval to use would be 1 hour (100,000 replication per hour).

Network data usage depends on the number of logs harvested by clients. In this test, this number was about 20 KB per replication, so 80 replications per second gives us about 1600 KB/s (20 Mbit/s) network speed.

In this example we used a single server scenario. CPU and network load will be better distributed when using multiple ERA Proxies (more is better). This will distribute both CPU load and network load when servicing client replications. It is good to distribute network load, particularly for clients in distant locations. Proxy replication interval to the server can be performed during non-working hours, when network speed from distant locations is better.

1.3 Supported products and languages

ESET Remote Administrator is able to deploy, activate or manage the following ESET products:

Manageable via ESET Remote Administrator 6	Product version	Activation method
ESET Endpoint Security for Windows	6.x & 5.x	6.x - License Key 5.x - Username/Password
ESET Endpoint Antivirus for Windows	6.x & 5.x	6.x - License Key 5.x - Username/Password
ESET Endpoint Security for OS X	6.x	License Key
ESET Endpoint Antivirus for OS X	6.x	License Key
ESET Endpoint Security for Android	2.x	License Key
ESET File Security for Windows Server	6.x	License Key
ESET File Security for Microsoft Windows Server	4.5.x	Username/Password
ESET NOD32 Antivirus 4 Business Edition for Mac OS X	4.x	Username/Password
ESET NOD32 Antivirus 4 Business Edition for Linux Desktop	4.x	Username/Password

Manageable via ESET Remote Administrator 6	Product version	Activation method
ESET Mail Security for Microsoft Exchange Server	4.5.x	Username/Password
ESET Mail Security for IBM Lotus Domino	4.5.x	Username/Password
ESET Security for Microsoft Windows Server Core	4.5.x	Username/Password
ESET Security for Microsoft SharePoint Server	4.5.x	Username/Password
ESET Security for Kerio	4.5.x	Username/Password
ESET NOD32 Antivirus Business Edition	4.2.76	Username/Password
ESET Smart Security Business Edition	4.2.76	Username/Password

NOTE: Versions of Windows Server products earlier than those shown in the table above are not currently manageable using ESET Remote Administrator.

Supported languages

Name	Code
English (United States)	en-US
Arabic (Egypt)	ar-EG
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Croatia)	hr-HR
Czech (Czech Republic)	cs-CZ
French (France)	fr-FR
French (Canada)	fr-FC
German (Germany)	de-DE
Italian (Italy)	it-IT
Japanese (Japan)	ja-JP
Korean (Korea)	ko-KR
Polish (Poland)	pl-PL
Portuguese (Brazil)	pt-BR
Russian (Russia)	ru-RU
Spanish (Chile)	es-CL
Spanish (Spain)	es-ES
Slovak (Slovakia)	sk-SK

2. System requirements

There is a set of hardware, database and software prerequisites which must be met in order to install ESET Remote Administrator.

2.1 Hardware

For seamless operation of ESET Remote Administrator, your system should meet the following hardware requirements:

Memory	4 GB RAM
Hard Drive	At least 20 GB of free space
Processor	Dual-Core, 2.0 GHz or faster
Network connection	1 Gbit/s

2.2 Database

ESET Remote Administrator supports two types of database servers:

- Microsoft SQL Server (including Express and non-Express editions) 2008, 2008 R2, 2012, 2014
- MySQL (version 5.5 and newer)

You can specify the database server that you want to use when you install the Server or the Proxy. Microsoft SQL Server 2008 R2 Express is installed by default and is a part of the installation package. Note that Microsoft SQL Server 2008 R2 Express has a 10 GB database size limit and cannot be installed on a Domain Controller, for example, if you use Microsoft SBS, we recommend that you install ESET Remote Administrator on a different server, or do not select the SQL Server Express component during installation (this requires you to use your existing SQL or MySQL Server to run the ERA database).

If you decide to use Microsoft SQL Server, the earliest supported version is **Microsoft SQL Server 2008**. You can use an existing Microsoft SQL Server running in your environment, but it must meet minimum requirements.

NOTE: ERA Server and ERA Proxy do not use an integrated backup, so we strongly recommend that you backup your database server to prevent data loss.

Database server hardware requirements:

Memory	1 GB RAM
Hard Drive	At least 10 GB of free space
Processor Speed	x86 Processor: 1.0 GHz x64 Processor: 1.4 GHz **Note**: A 2.0 GHz or faster processor is recommended for optimum performance.
Processor Type	x86 Processor: Pentium III-compatible processor or faster x64 Processor: AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support

2.3 Supported Operating Systems

The following sections describe which operating system versions are supported under Windows, Linux and Mac OS by particular component of ESET Remote Administrator.

2.3.1 Windows

The following table displays supported operating systems for each ESET Remote Administrator component. It is also possible to install ERA Server, ERA Proxy and MDM on a client operating system (*Microsoft Windows 7, 8 , 8.1) for **evaluation purposes only**.

Operating System	Server	Agent	Proxy	RD Sensor	MDM
Windows XP x86 SP3		X		X	
Windows XP x64 SP2		X		X	
Windows Vista x86 SP2		X		X	
Windows Vista x64 SP2		X		X	
Windows 7 x86 SP1	*	X	*	X	*
Windows 7 x64 SP1	*	X	*	X	*
Windows 8 x86	*	X	*	X	*
Windows 8 x64	*	X	*	X	*
Windows 8.1 x86	*	X	*	X	*
Windows 8.1 x64	*	X	*	X	*
Windows HomeServer 2003 SP2		X		X	
Windows HomeServer 2011 x64		X		X	
Windows Server 2003 x86 SP2	X	X	X	X	
Windows Server 2003 x64 SP2	X	X	X	X	
Windows Server 2003 x86 R2 SP2	X	X	X	X	
Windows Server 2003 x64 R2 SP2	X	X	X	X	
Windows Server 2008 x64 R2 SP1	X	X	X	X	X
Windows Server 2008 x64 R2 CORE	X	X	X	X	X
Windows Server 2008 x86		X		X	
Windows Server 2008 x86 SP2	X	X	X	X	X
Windows Server 2008 x64		X		X	
Windows Server 2008 x64 SP2	X	X	X	X	X
Windows Server 2012 x64	X	X	X	X	X
Windows Server 2012 x64 CORE	X	X	X	X	X
Windows Server 2012 x64 R2	X	X	X	X	X
Windows Server 2012 x64 R2 CORE	X	X	X	X	X
Microsoft SBS 2003 x86 SP2 **	X	X	X	X	X
Microsoft SBS 2003 x86 R2 **	X	X	X	X	X
Microsoft SBS 2008 x64		X		X	
Microsoft SBS 2008 x64 SP2 **	X	X	X	X	X
Microsoft SBS 2011 x64 Standard	X	X	X	X	X
Microsoft SBS 2011 x64 Essential	X	X	X	X	X

*** ERA components running on client operating systems (for evaluation purpose only).**

**** Microsoft SQL Server Express included with Microsoft Small Business Server (SBS) is not supported by ESET Remote Administrator**. If you want to run your ERA database on SBS, you must use a newer version of Microsoft SQL Server. For more details and instructions see Installation on Windows SBS / Essentials**.**

On older systems, for example Windows Server 2003, protocol encryption might not be fully supported on the operating system side. Therefore, TLSv1.0 will be used instead of TLSv1.2, (TLSv1.0 is considered to be less secure than more recent versions). This situation can also occur when the operating system supports TLSv1.2 but the client does not. In this case, communication takes place using TLS1.0. If you require more secure communication, we suggest that you use newer operating systems and clients (Windows Server 2008 R2 and later for servers and Windows Vista and later for clients).

NOTE: It is possible to install VMware Player on a desktop Operating System and deploy Virtual appliance. This lets you run ESET Remote Administrator on a non-server OS without the need for ESXi.

2.3.2 Linux

Operating System	Server	Agent	Proxy	RD Sensor	MDM
Ubuntu 12.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x86 Server	X	X	X	X	X
Ubuntu 12.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x64 Server	X	X	X	X	X
Ubuntu 14.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x86 Server	X	X	X	X	X
Ubuntu 14.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x64 Server	X	X	X	X	X
RHEL 5 x86		X			
RHEL 5 x64		X			
RHEL Server 6 x86	X	X	X	X	X
RHEL Server 6 x64	X	X	X	X	X
RHEL Server 7 x86	X	X	X	X	X
RHEL Server 7 x64	X	X	X	X	X
CentOS 5 x86		X			
CentOS 5 x64		X			
CentOS 6 x86	X	X	X	X	X
CentOS 6 x64	X	X	X	X	X
CentOS 7 x86	X	X	X	X	X
CentOS 7 x64	X	X	X	X	X
SLED 11 x86	X	X	X	X	X
SLED 11 x64	X	X	X	X	X
SLES 11 x86	X	X	X	X	X
SLES 11 x64	X	X	X	X	X
OpenSUSE 13 x86	X	X	X	X	X
OpenSUSE 13 x64	X	X	X	X	X
Debian 7 x86	X	X	X	X	X
Debian 7 x64	X	X	X	X	X
Fedora 19 x86	X	X	X	X	X
Fedora 19 x64	X	X	X	X	X
Fedora 20 x86	X	X	X	X	X
Fedora 20 x64	X	X	X	X	X

2.3.3 OS X

Operating System	Agent
OS X 10.7 Lion	X
OS X 10.8 Mountain Lion	X
OS X 10.9 Mavericks	X
OS X 10.10 Yosemite	X

NOTE: OS X is supported as a client only. ERA Server can not be installed on OS X.

2.4 Ports used

The charts below lists all possible network communication ports used when ESET Remote Administrator and its components are installed in your infrastructure. Other communication occurs via the native operating system processes (for example NetBIOS over TCP/IP).

ERA Server:

Protocol	Port	Usage	Descriptions
TCP	2222	ERA Server listening	Communication between ERA Agents andERA Server
TCP	2223	ERA Server listening	Communication between ERA Web Console and ERA Server, used for Assisted installation

ERA Web Console web server:

Protocol	Port	Usage	Descriptions
TCP	443	Listening	HTTP SSL Web Console call

ERA Proxy:

Protocol	Port	Usage	Descriptions
TCP	2222	Listening	Communication between ERA Agents and ERA Proxy

HTTP Proxy:

Protocol	Port	Usage	Descriptions
TCP	3128	Listening	HTTP Proxy (update caching)

ERA Agent:

Protocol	Port	Usage	Descriptions
UDP	1237	Listening	Wake-up call

Mobile Device Connector:

Protocol	Port	Usage	Descriptions
TCP	9980	Mobile device enrollment	Enrollment port
TCP	9981	Communication with ERA	Mobile Device Connector connects to ERA Server

ERA Agent - used for remote deployment of ERA Agent to a target computer with Windows OS:

Protocol	Port	Usage	Descriptions
TCP	139	Target port from the point of view of ERA Server	Using the share ADMIN$
TCP	445	Target port from the point of view of ERA Server	Direct access to shared resources using TCP/IP during remote installation (an alternative to TCP 139)
UDP	137	Target port from the point of view of ERA Server	Name resolution during remote install
UDP	138	Target port from the point of view of ERA Server	Browse during remote install

The pre-defined ports 2222, 2223 can be changed if they are already in use by other applications.

NOTE: All the ports above must not be used by other applications. Otherwise, you might experience issues because of that.

NOTE: Make sure to configure firewall(s) within your network to allow for communication via the ports listed above.

3. Installation process

ESET Remote Administrator installation can be performed in a few different ways. Choose the type of installation that best suits your needs and environment. The simplest method, ESET Remote Administrator (ERA) installer (All-in-one package installation) allows you to install ESET Remote Administrator and its components on a single machine. Component installation allows for the installation of different components of ESET Remote Administrator on different machines. This gives you more freedom to customize your installation - you can install each component on any machine you want, provided that it meets system requirements. Deployment to a Virtual Appliance is available for users who want to run ERA in a virtualized environment.

The ESET Remote Administrator installers are available in different forms. They are available in the download section of the ESET website under **Remote Management** (click the + sign to expand the category). Here, you can download the following:

- The ERA Installer package in a zipped form
- Separate installers for each component
- Virtual appliance (OVA file)
- An ISO image that contains all installers of ESET Remote Administrator (including the above)

To install ESET Remote Administrator, follow these steps:

1. Make sure that all Requirements are satisfied.
2. Choose either Package installation (All-in-one ERA installer) or Component installation on your Windows or Linux operating system. Alternatively, you can use Virtual appliance by deploying OVA file.
3. Download appropriate installer, either installer package for package installation, or separate installers for each component you plan to install. You can also download virtual appliance OVA file or an ISO image that contains all installers of ESET Remote Administrator.
4. Perform the installation according to the installation instructions that are covered in next chapters.
5. If necessary, install optional components (ERA Proxy server, RD Sensor, Mobile Device Connector)

Once you finish the installation process, you can connect to the ERA Server using the ERA Web Console and take the first steps to configure it in order to start using ESET Remote Administrator.

3.1 Package installation

Package installation of ERA (All-in-one installer) is only available for Windows operating systems, and is a convenient way to install all ERA components using a simple installation wizard. When you run the installation package, you will be given two options:

- Remote Administrator Server installation
- Remote Administrator Proxy installation

Remote Administrator Server installation

Use the written instructions below, watch our Knowledgebase instructional video, or visit our Knowledgebase article for illustrated step-by-step instructions to complete installation using the All-in-one installer.

1. Double-click the installation package to begin installation. Select **Remote Administrator Server**.

NOTE: If you want to install ERA in a Failover Cluster environment, a component installation is required.

2. Select the components that you want to install. If you do not have a database server, you can install Microsoft SQL Server 2008 R2 Express, which is included in the installation package. Note that Microsoft SQL Server 2008 R2 Express has a 10 GB database size limit. You can also install the ERA Web Console, Mobile Device Connector, Apache HTTP Proxy and Rogue Detection Sensor using the package installation method.
3. Enter a valid License Key or choose **Activate Later**.

4. If you are using a SQL Express database, the connection to the database will be verified and you will be prompted to enter a password for the ERA Web Console (Step 8), as well as your Certificate password (Step 10).
5. If you are using a different database system: Select **Service user account**. This account will be used to run the ESET Remote Administrator Server Service. The options available are:
    a. Network service account
    b. User specified: DOMAIN/USERNAME
6. Connect to a Database. All data is stored here, from the Web Console password to client computer logs.
    a. Database: MySQL/MS SQL
    b. ODBC Driver: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/SQL Server
    c. Hostname: Hostname or the IP Address of the database server
    d. The port used for connection with the Server
    e. DB Admin username/password

This step will verify your connection to the database. If the connection is ok, you can proceed to the next step.

7. Select a user for ESET Remote Administrator that has access to the database. You can use an existing user or create a new one.
8. Enter a password for **Web Console** access.
9. ESET Remote Administrator uses certificates for client-server communication. You can either select your own certificates, or the **Server** can create new certificates for you.
10. Define a password for your **Certification authority. Be sure to remember this password!** To create a Certificate Authority for ESET Remote Administrator, click **Next**. Optionally, specify additional information about the certificate (this is not mandatory). You can leave the **Authority password** field empty, but if you enter the password, **be sure to remember it**.
11. Click **Install** to install the ERA Server.
12. When installation finishes, click the link displayed in the Setup wizard to open the Web Console (we recommend that you bookmark this URL) and then click **Finish**.

NOTE: If installation ends with the error 2068052081, see our FAQ for solutions.

Remote Administrator Proxy installation

1. Start the installation package. Select **Remote Administrator Proxy**.
2. Select the components that you want to install. If you do not have a database server, you can install Microsoft SQL Server 2008 R2 Express, which is included in the installation package. Note that Microsoft SQL Server 2008 R2 Express has a 10 GB database size limit.You can also install the RD Sensor from the installation package.
3. Connect to a Database:
    a. Database: MySQL/MS SQL
    b. ODBC Driver: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/SQL Server
    c. Hostname: The hostname or IP Address of the database server
    d. Port used for connection with the Server
    e. DB Admin username/password

This step will verify your connection to the database. If the connection is ok, you can proceed to the next step.

4. Select a proxy communication port. By default, port 2222 is used.
5. Configure the proxy connection to ESET Remote Administrator. Enter a **Server host** (hostname/ip address of the Server) and **Server port** (2222).
6. Select a Peer Certificate and a password for this certificate. Optionally, add a Certificate Authority. This is only needed for unsigned certificates.

7. Optionally, select a folder where the Proxy will be installed and click **Install**.
8. The ERA Agent will be installed in addition to the Proxy.

3.1.1 Installation on Windows SBS / Essentials

Make sure that all Requirements are met, especially Supported Operating System.

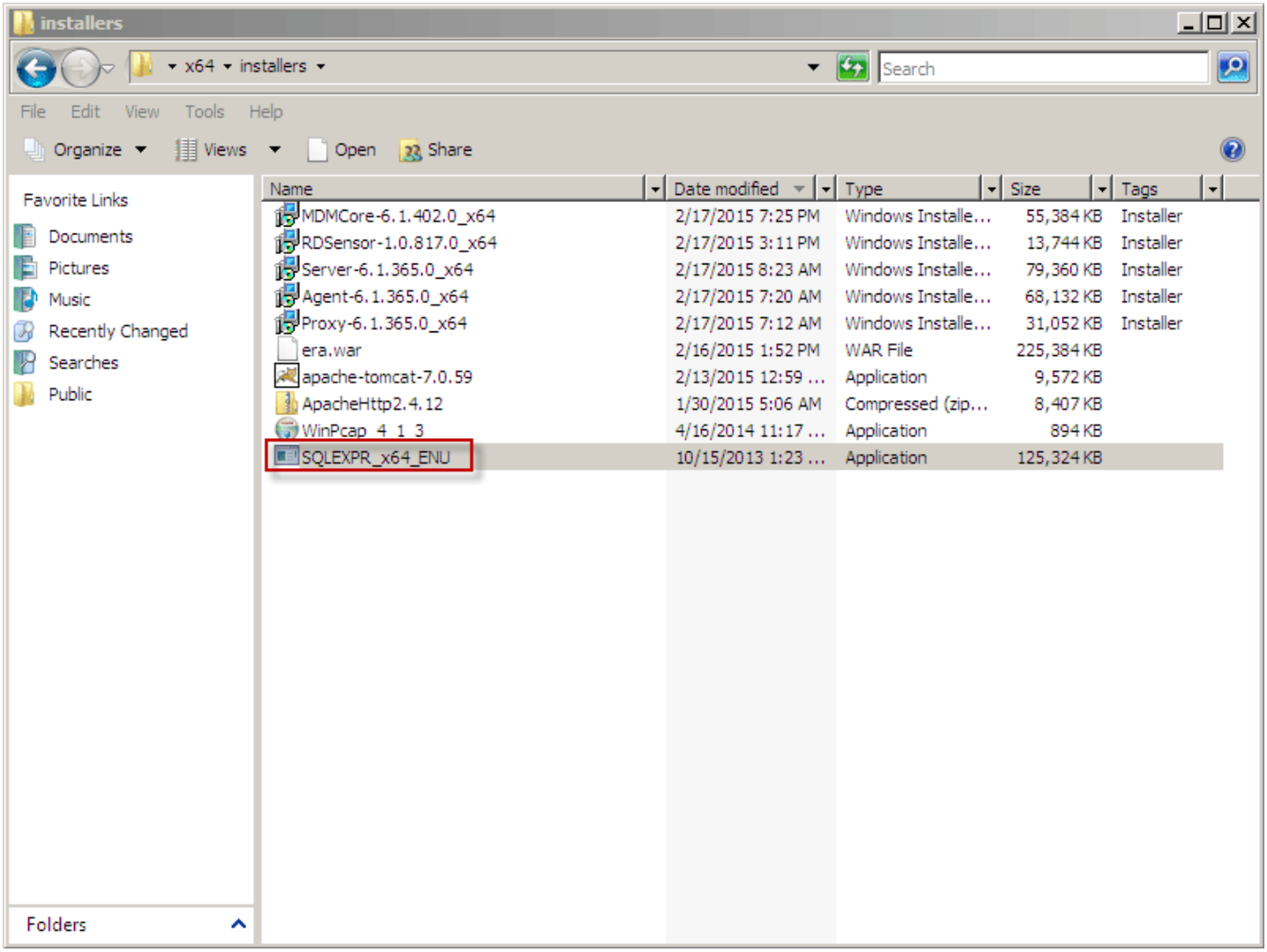
NOTE: Some older Microsoft SBS versions include versions of Microsoft SQL Server Express not supported by ESET Remote Administrator:

Microsoft SBS 2003 x86 SP2
Microsoft SBS 2003 x86 R2
Microsoft SBS 2008 x64 SP2

If you have any of the above versions of Windows Small Business Server and want to install the ERA database on Microsoft SBS, you must use a newer version of Microsoft SQL Server Express.

- If you do not have Microsoft SQL Express installed on your SBS, follow the steps below.
- If you do have Microsoft SQL Express installed on your SBS but are not using it, uninstall it and follow the steps below.
- If you are using the version of Microsoft SQL Server Express that came with SBS, migrate your database to a version of SQL Express compatible with ERA Server. To do so, back up your databases, uninstall your previous installation of Microsoft SQL Server Express and follow the steps below to install a compatible version of Microsoft SQL Server Express and restore databases if required.

1. Download the ERA Installer package in a zipped form from the download section of the ESET website under **Remote Management** (click **+** to expand the category).
2. Unzip the installer file you downloaded in step one, open the **installers** folder and double-click **SQLEXPR_x64_ENU**.

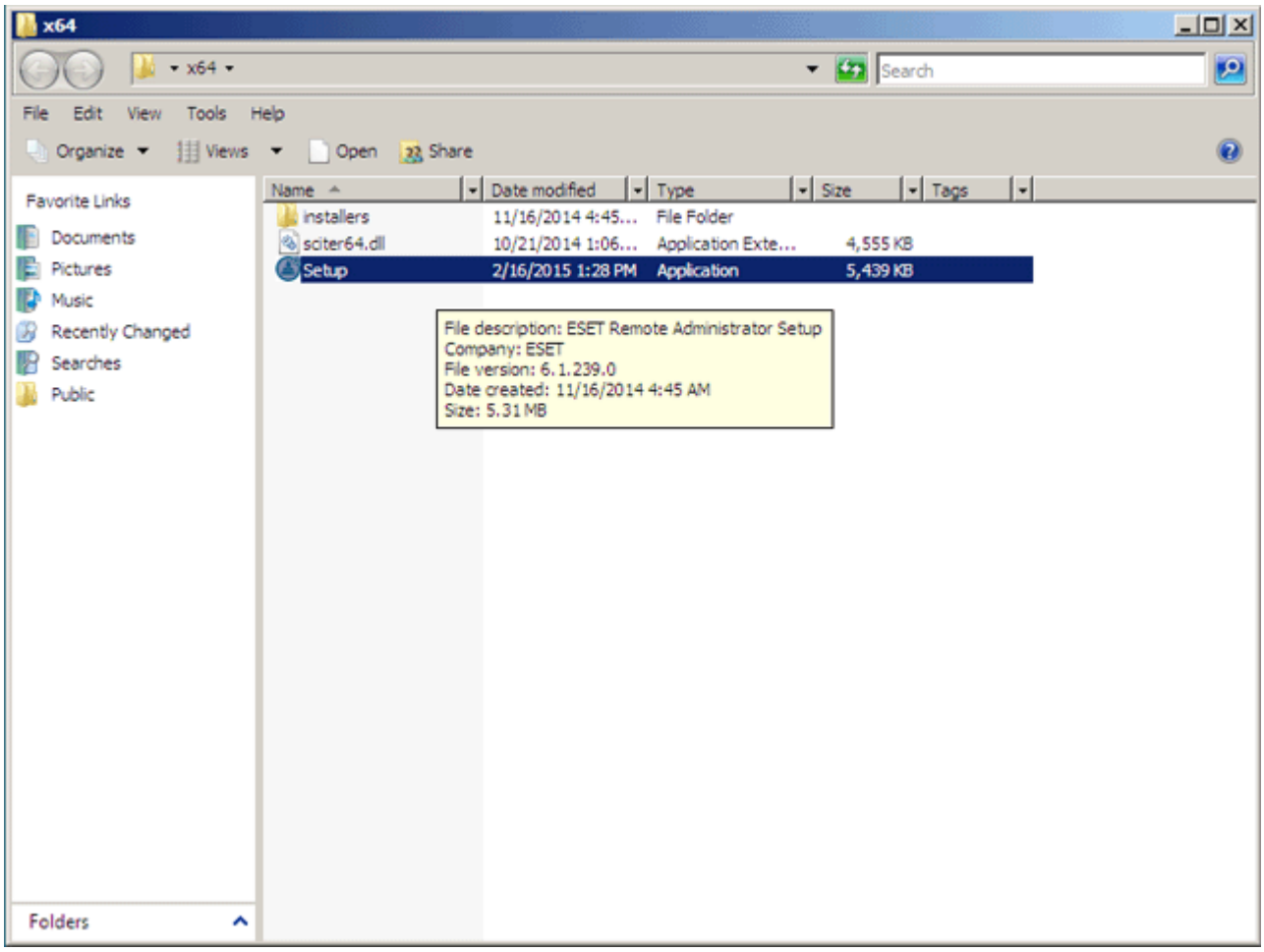

installers
x64 ▸ installers
Search
File Edit View Tools Help
Organize Views Open Share
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders
Name
Date modified
Type
Size
Tags
MDMCore-6.1.402.0_x64 2/17/2015 7:25 PM Windows Installe... 55,384 KB Installer
RDSensor-1.0.817.0_x64 2/17/2015 3:11 PM Windows Installe... 13,744 KB Installer
Server-6.1.365.0_x64 2/17/2015 8:23 AM Windows Installe... 79,360 KB Installer
Agent-6.1.365.0_x64 2/17/2015 7:20 AM Windows Installe... 68,132 KB Installer
Proxy-6.1.365.0_x64 2/17/2015 7:12 AM Windows Installe... 31,052 KB Installer
era.war 2/16/2015 1:52 PM WAR File 225,384 KB
apache-tomcat-7.0.59 2/13/2015 12:59 ... Application 9,572 KB
ApacheHttp2.4.12 1/30/2015 5:06 AM Compressed (zip... 8,407 KB
WinPcap_4_1_3 4/16/2014 11:17 ... Application 894 KB
SQLEXPR_x64_ENU 10/15/2013 1:23 ... Application 125,324 KB

- The Installation Center will launch, click **New installation or add features to an existing installation** to start the Installation Wizard.

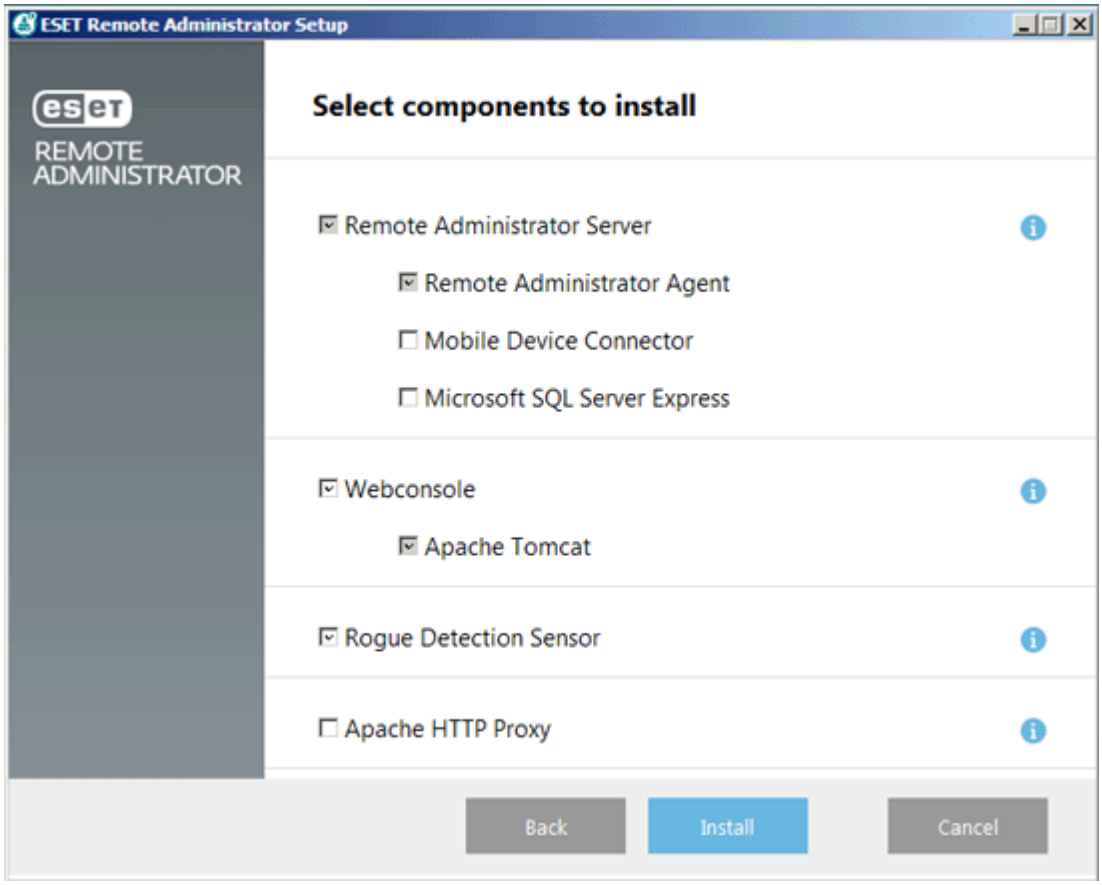
NOTE: In step 8 of the installation process set the Authentication mode to **Mixed mode (SQL Server authentication and Windows authentication)**.

NOTE: To install ERA Server on SBS, you must allow TCP/IP connections to the SQL Server.

3. Install ESET Remote Administrator by running **Setup.exe**.



4. Select the components you want to install, make sure to deselect **Microsoft SQL Server Express** and click **Install**.



3.2 Database

ESET Remote Administrator uses a database to store client data. The following sections detail the installation, backup, upgrade and migration of the ERA Server/ERA Proxy database:

- Review database compatibility and system requirements for ERA Server.
- If you do not have a database configured for use with ERA Server, **Microsoft SQL Server Express** is included with the installer.
- If you use Microsoft Small Business Server (SBS) or Essentials, we recommended that you make sure all requirements are met and that you are using a supported Operating System. When all requirements are met, follow the installation instructions for Windows SBS / Essentials to install ERA on these operating systems.
- If you have Microsoft SQL Server installed in your system, review the requirements to make sure your version of Microsoft SQL Server is supported by ESET Remote Administrator. If your version of Microsoft SQL Server is not supported, upgrade to a compatible version of SQL Server.

3.2.1 Database Server Backup

All ESET Remote Administrator information and settings are stored in the database. We recommend that you back up your database regularly to prevent loss of data. Refer to the appropriate section below for your database:

- MySQL
- SQL Server

The backup can also be used later when migrating ESET Remote Administrator to a new server.

If you want to restore the database backup, follow these instructions:

- MySQL
- SQL Server

3.2.2 Database Server Upgrade

Follow the instructions below to upgrade an existing Microsoft SQL Server instance to a newer version for use with ERA Server or ERA Proxy database:

1. **Stop** all running ERA Server or ERA Proxy services connecting to the database server that you will be upgrading. Additionally, stop any other applications that might be connecting to your Microsoft SQL Server instance.
2. Back up all relevant databases safely before proceeding.
3. Perform the database server upgrade following the database vendor's instructions.
4. **Start** all ERA Server and or ERA Proxy services and check their trace logs to verify the database connection is working correctly.

See the following web pages for more information specific to your database:

- Upgrade SQL Server https://msdn.microsoft.com/en-us/library/bb677622.aspx (you can click **Other Versions** for instructions to upgrade to a specific SQL Server version)
- Upgrade MySQL Server (to version 5.6) http://dev.mysql.com/doc/refman/5.6/en/upgrading.html

3.2.3 ERA Database Migration

Click the appropriate link below for instructions to migrate ERA Server or ERA Proxy database between different SQL Server instances (this also applies when migrating to a different SQL Server version or when migrating to a SQL Server hosted on a different machine):

- Migration process for SQL Server
- Migration process for MySQL Server

3.2.3.1 Migration process for SQL Server

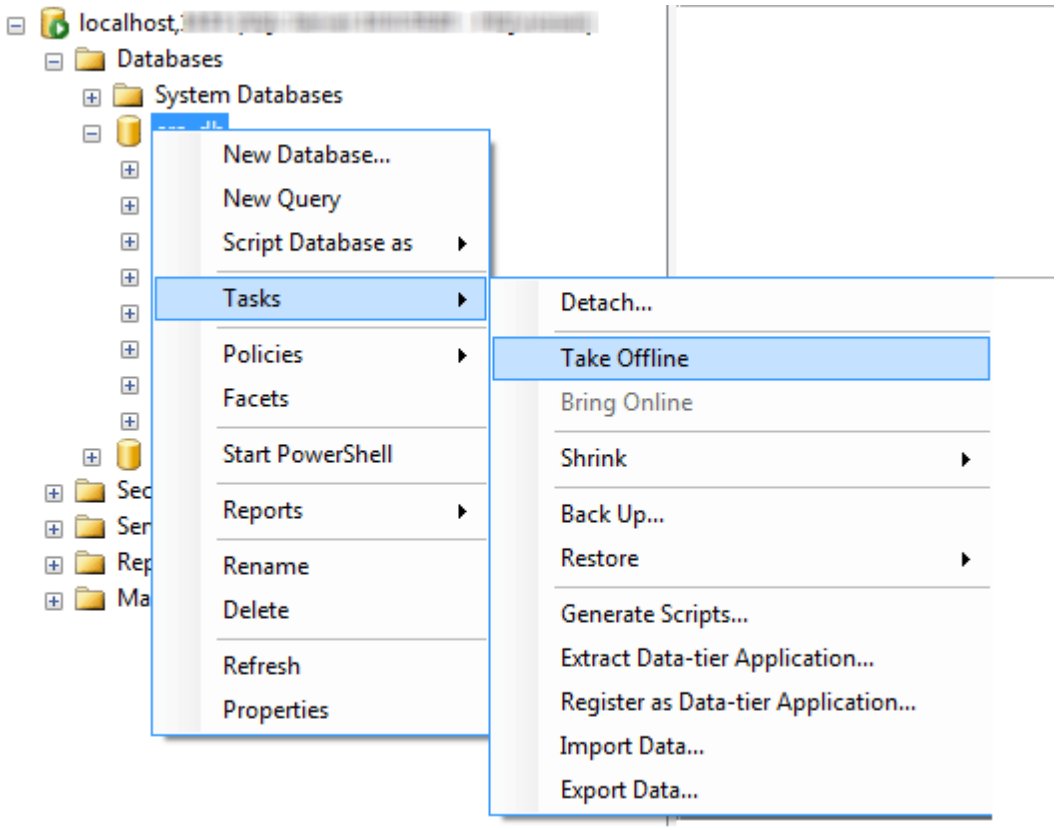
This migration process is the same for **Microsof SQL Server** and **Microsoft SQL Server Express**.

For additional information, see the following Microsoft Knowledge Base article: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

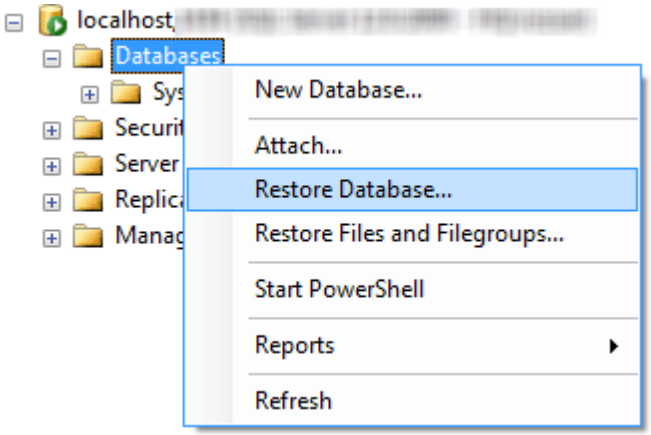
- **Prerequisites:**
  - Source and target SQL Server instances must be installed. They may be hosted on different machines.
  - The target SQL Server instance must have at least the same version as the source instance. **Downgrade is not supported!**
  - **SQL Server Management Studio** must be installed. If the SQL Server instances are on different machines, it must be present on both.

- **Migration:**

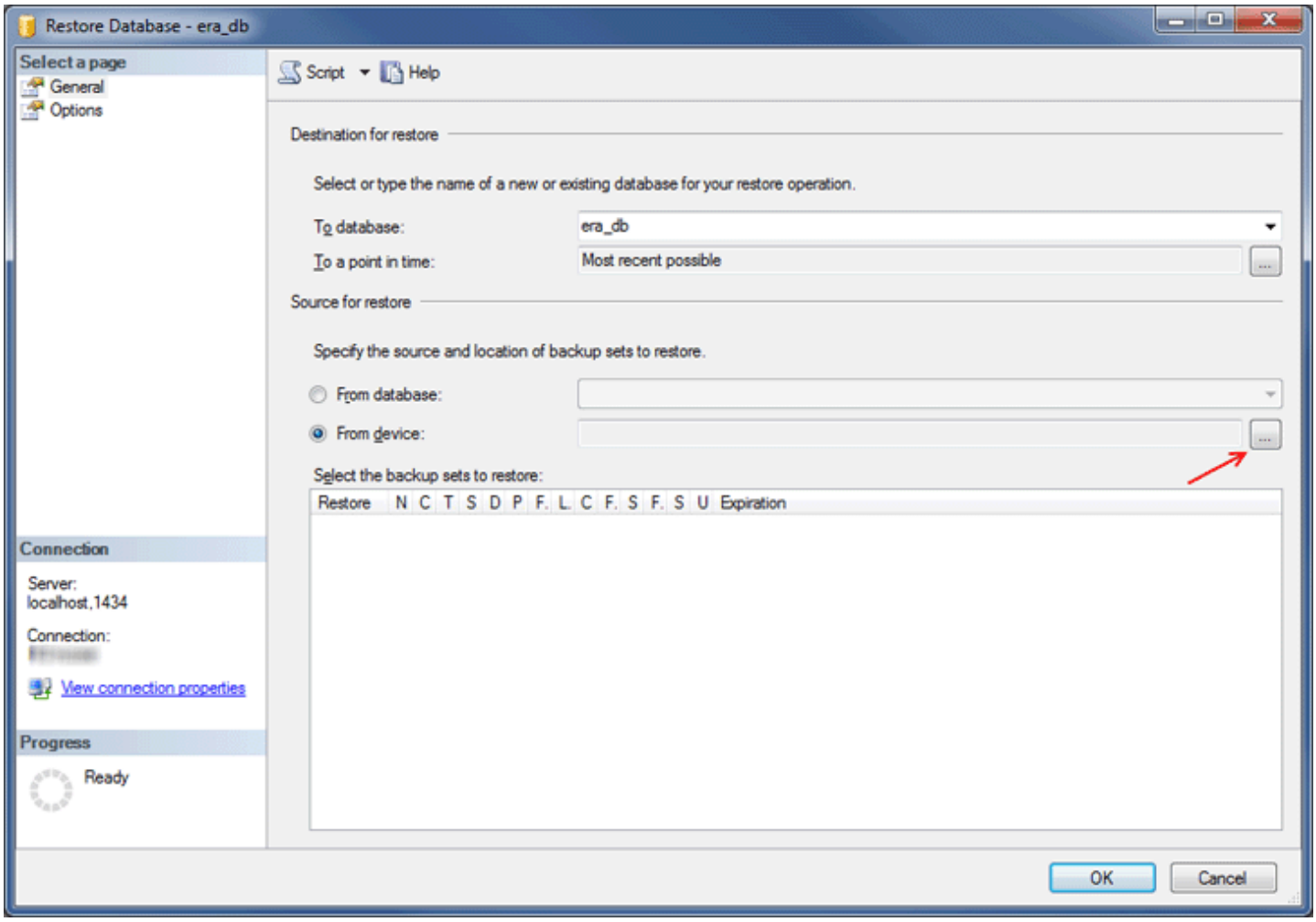
1. **Stop** the ERA Server or ERA Proxy Service.
2. Log into the source SQL Server instance via SQL Server Management Studio.
3. **Create** a full database backup of the database to be migrated. We recommend that you specify a new backup set name. Otherwise if the backup set has already been used, the new backup will be appended to it, which will result in an unnecessarily large backup file.
4. Take the source database offline, select **Tasks** > **Take Offline**.



5. **Copy** the backup (.bak) file that you created in step 3 to a location that is accessible from the target SQL Server instance. You may need to edit access rights for the database backup file.
6. **Bring** the source database online again but **do not start ERA Server yet!**
7. Log into the target SQL Server instance with SQL Server Management Studio.
8. Restore your database on the target SQL Server instance.



9. Type a name for your new database into the **To database** field. You can use the same name as your old database if your prefer**.**
10. Select **From device** under **Specify the source and location of backup sets to restore** and then click **…** .

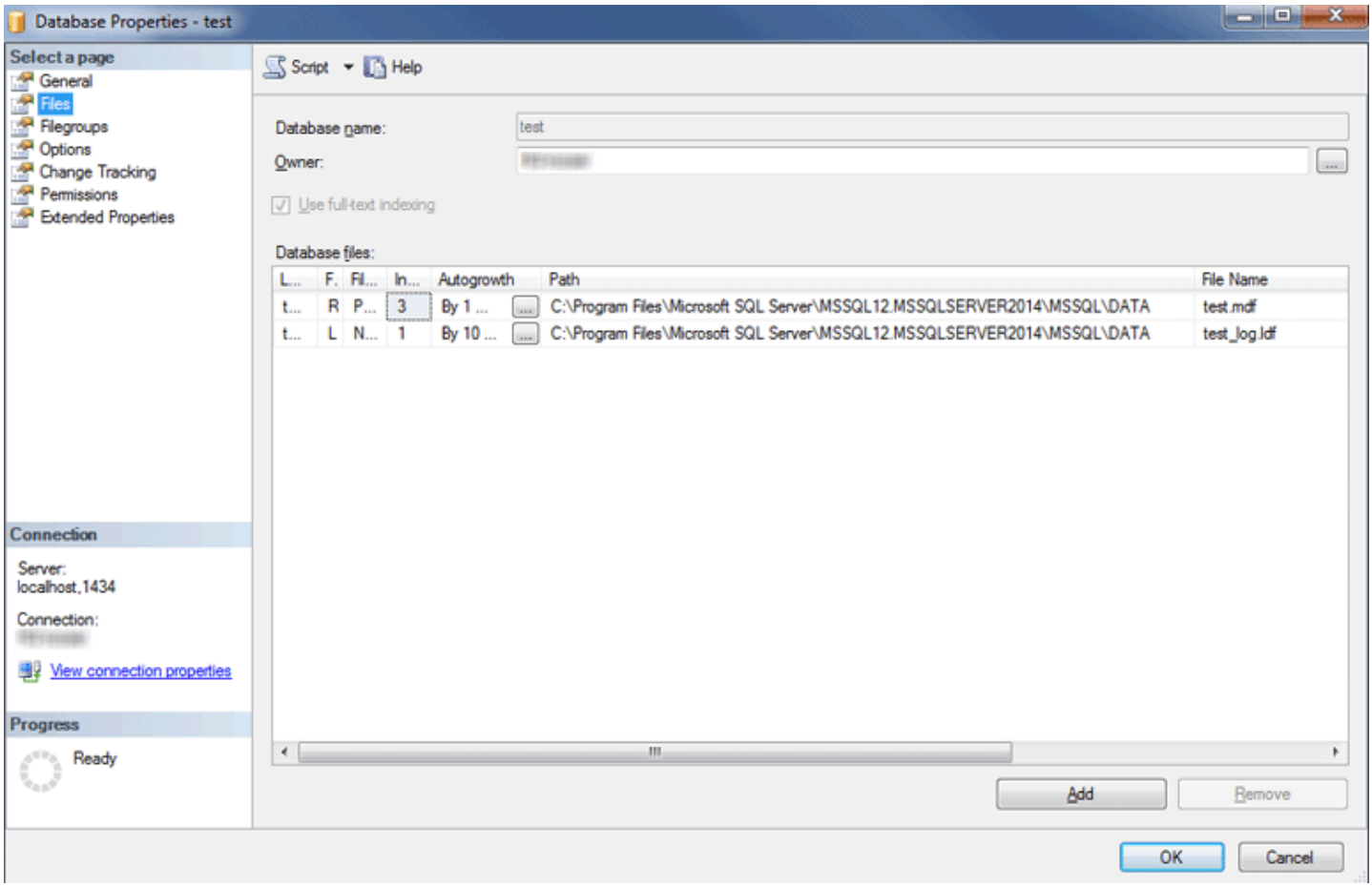


11. Click **Add**, navigate to your backup file and then open it.

12. Select the most recent possible backup to restore (the backup set may contain multiple backups).

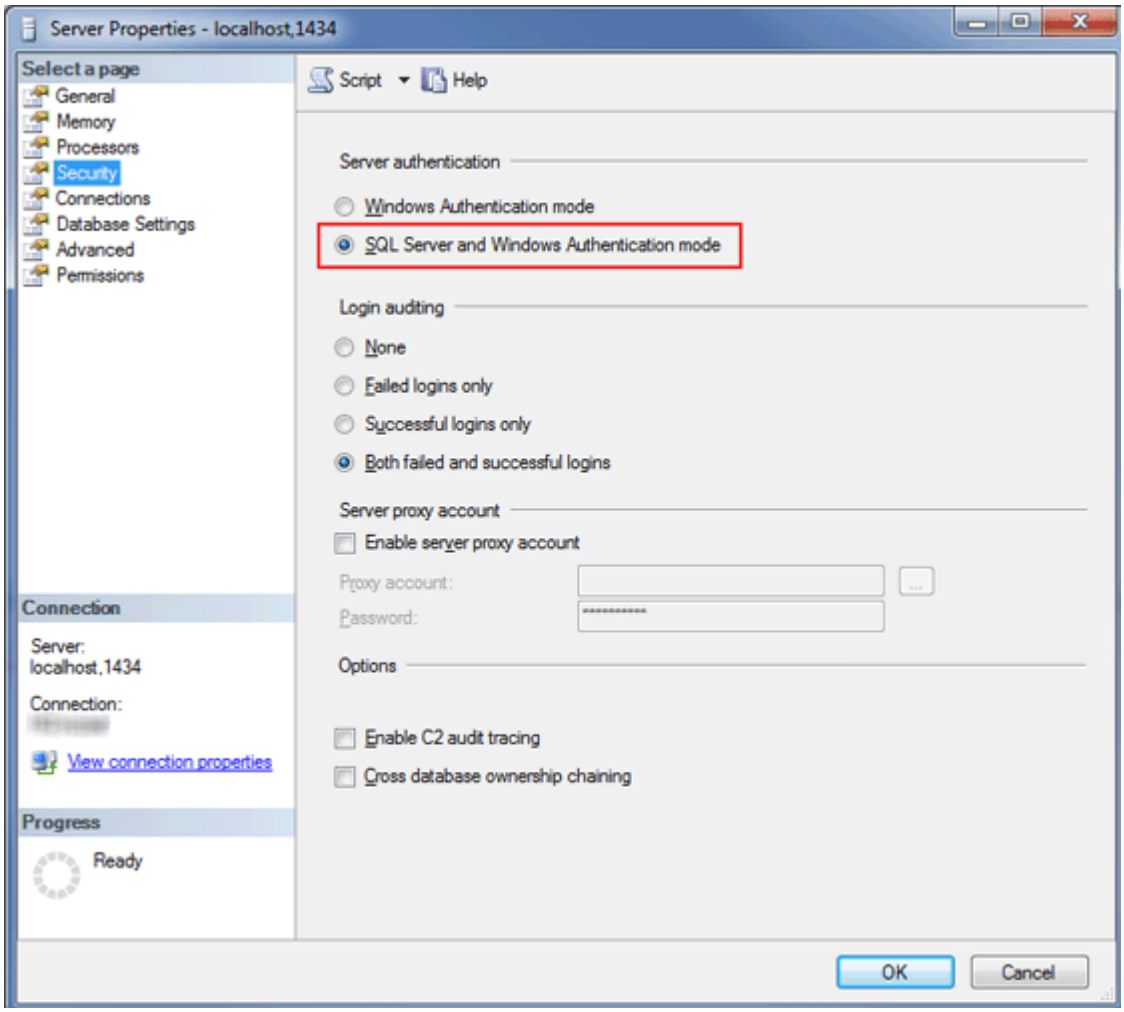
13. Click the **Options** page of the restore wizard. Optionally, select **Overwrite existing database** and ensure that the restore locations for the database (`.mdf`) and for the log (`.ldf`) are correct. Leaving the default values unchanged will use the paths from your source SQL server, so please check these values.

    - If you are unsure where the DB files are stored on the target SQL Server instance, right-click an existing database, select **properties** and click the **Files** tab. The directory where the database is stored is displayed in the **Path** column of the table shown below.



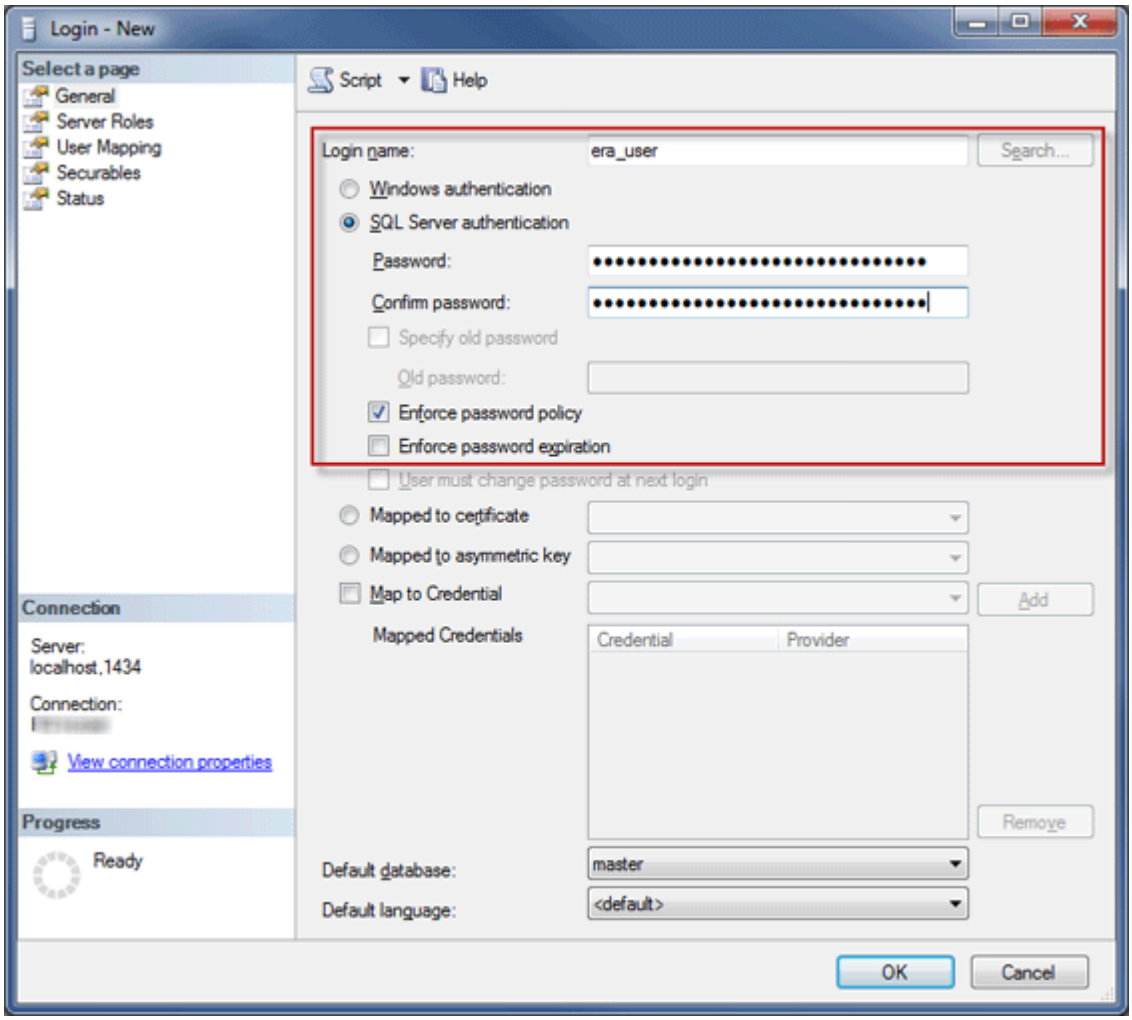
14. Click **OK** in the restore wizard window.

15. Ensure that the new database server has **SQL Server Authentication enabled**. Right-click the server and click **Properties**. Navigate to **Security** and verify that **SQL Server and Windows Authentication mode** is selected.

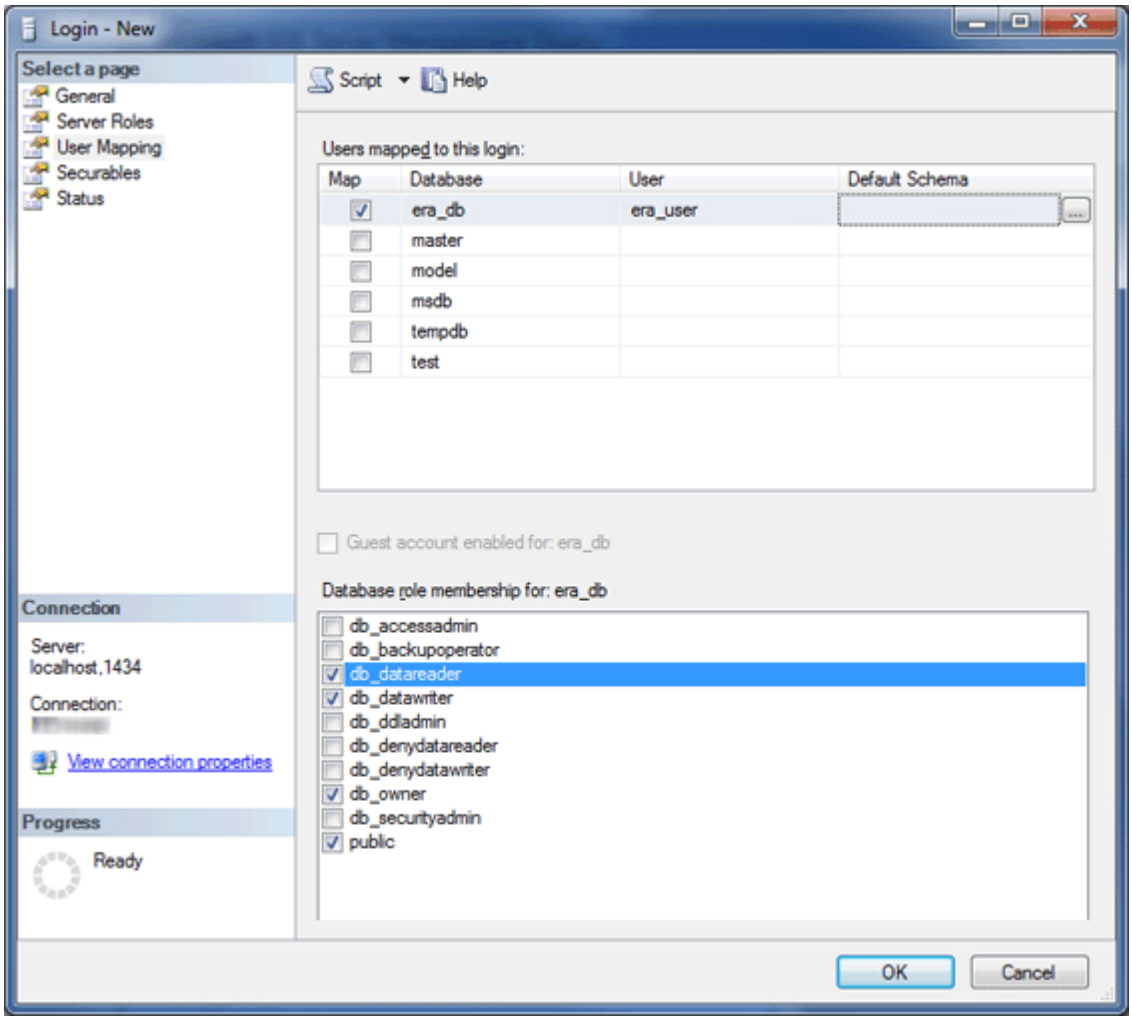


16. **Create a new SQL Server login** (for ERA Server/Proxy) in the target SQL Server with **SQL Server authentication** and map the login to a user in the restored database.

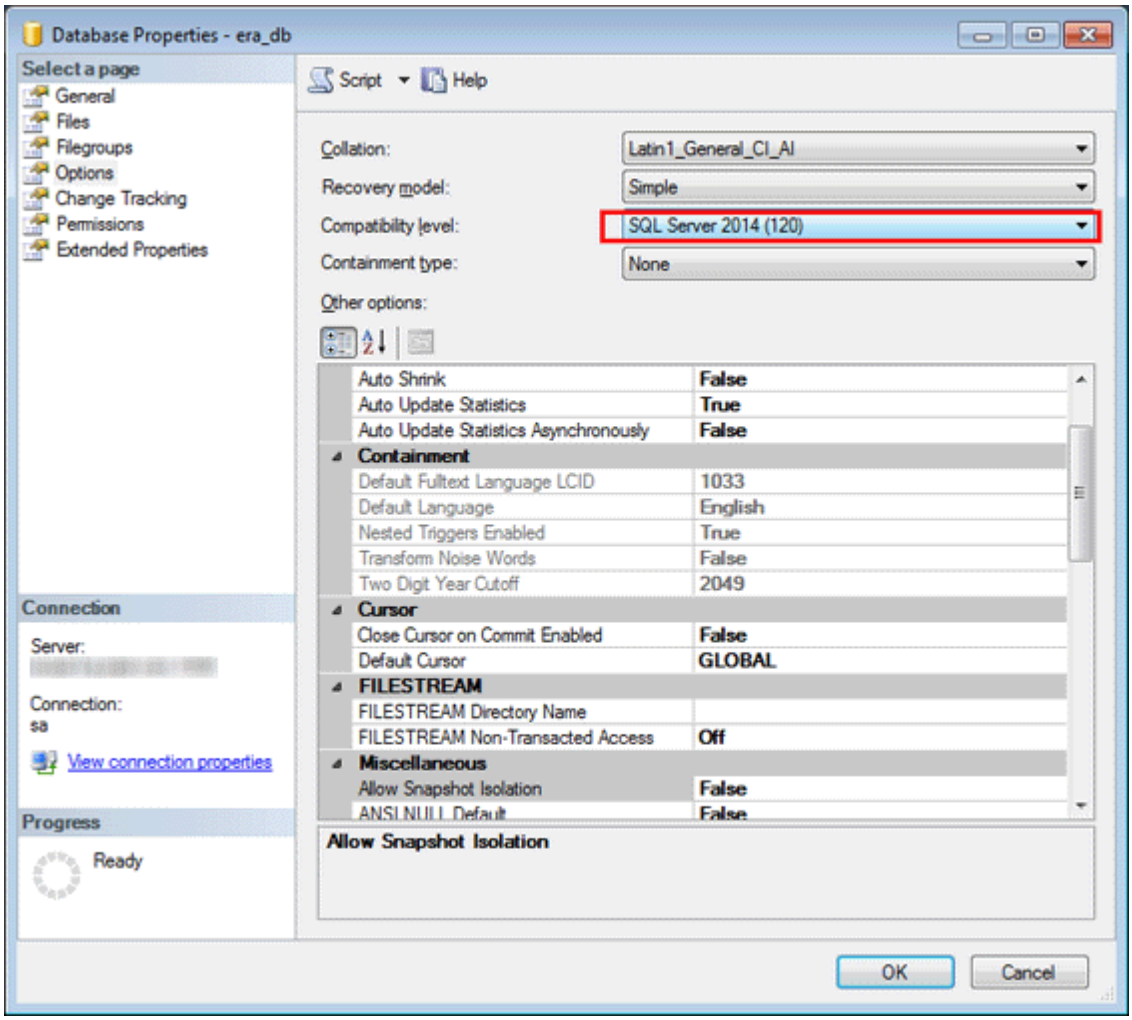
- Do not enforce password expiration!
- Recommended characters for usernames:
  - Small ASCII letters, numbers and character underscore "_"
- Recommended characters for passwords:
  - ASCII characters ONLY, including big and small ASCII letters, numbers, spaces, special characters
- Do not use non-ASCII characters, curly braces {} or @
- Please note that if you do not follow the character recommendations above, you may have database connectivity problems or you will need to escape the special characters in the later steps during database connection string modification. Character escaping rules are not included in this document.



17. Map the login to a user in the target database. In the **user mappings** tab, ensure that the database user has the roles: **db_datareader**, **db_datawriter**, **db_owner**.



18.To enable the latest database server features, change the restored database **Compatibility level** to the newest. Right-click the new database and open the database **Properties**.



NOTE: SQL Server Management Studio is unable to define compatibility levels later than that of the version in use. For example SQL Server Management Studio 2008 is unable to set compatibility level for SQL Server 2014.

19. **Find** `startupconfiguration.ini` on the machine, where ERA Server/Proxy is installed.

   - For Windows Vista and later:
     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - For earlier Windows versions:
     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - For Linux:
     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

20. **Change** the database connection string in ERA Server/Proxy startupconfiguration.ini

   - Set the address and port of the new database server.
   - Set new ERA user name and password in the connection string.
     - The final result should look like:

```
DatabaseType=MSSQLOdbc
DatabaseConnectionString=Driver=SQL Server;Server=localhost,1433;Uid=era_user1;Pwd={SecretPassword123
```

21. **Start** the ERA Server/Proxy and verify that the ERA Server/Proxy service is running correctly.

3.2.3.2 Migration process for MySQL Server

- **Prerequisites:**
  - Source and target SQL Server instances must be installed. They may be hosted on different machines.
  - MySQL tools must be available on at least one of the computers (mysqldump and mysql client).

- **Useful links:**

http://dev.mysql.com/doc/refman/5.6/en/copying-databases.html

http://dev.mysql.com/doc/refman/5.6/en/mysqldump.html

http://dev.mysql.com/doc/refman/5.6/en/mysql.html

- In the commands, configuration files or SQL statements below, please always replace:
  - **SRCHOST** with the address of the source database server
  - **SRCROOTLOGIN** with the source MySQL server root user login
  - **SRCERADBNAME** with the name of the source ERA database to back up
  - **BACKUPFILE** with the path to the file where the backup will be stored
  - **TARGETHOST** with the address of the target database server
  - **TARGETROOTLOGIN** with the target MySQL server root user login
  - **TARGETERADBNAME** with the name of the target ERA database (after migration)
  - **TARGETERALOGIN** with the login name for the new ERA database user on the target MySQL server
  - **TARGETERAPASSWD** with the password of the new ERA database user on the target MySQL server

It is not necessary to execute the SQL statements below via the command line. If there is GUI tool available, you can use an application you already know.

1. **Stop** the ERA Server/Proxy services.
2. **Create** a full database backup of the source ERA database (the database you plan to migrate):
```
mysqldump --host SRCHOST --disable-keys --extended-insert -u SRCROOTLOGIN -p SRCERADBNAME > BACKUPFILE
```
3. **Prepare** an empty database on the target MySQL server:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE DATABASE TARGETERADBNAME /*!40100 DEFAULT
```

NOTE: Use the apostrophe character ' instead of " quotation marks on Linux systems.

4. **Restore** the database on the target MySQL server to the previously prepared empty database:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETERADBNAME < BACKUPFILE
```
5. **Create** an ERA database user on the target MySQL server:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE USER TARGETERALOGIN@'%' IDENTIFIED BY 'TA
```

Recommended characters for **TARGETERALOGIN**:
- Small ASCII letters, numbers and underscore "_"

Recommended characters for **TARGETERAPASSWD**:
- ASCII characters only, including large and small ASCII letters, numbers, spaces and special characters
- Do not use non-ASCII characters, curly braces {} or @

Please note that if you do not follow the character recommendations above, you may have database connectivity problems or you will need to escape the special characters in the later steps during database connection string modification. Character escaping rules are not included in this document**.**

6. **Grant** proper access rights for the ERA database user on the target MySQL server:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=GRANT ALL ON TARGETERADBNAME.* TO TARGETERALOGIN
```

NOTE: Use the apostrophe character ' instead of " quotation marks on Linux systems.

7. **Find** `startupconfiguration.ini` on the machine where ERA Server/Proxy is installed.
   - For Windows Vista and later:
     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - For earlier Windows versions:
     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - For Linux:
     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
8. **Change** the database connection string in ERA Server/Proxy `startupconfiguration.ini`
   - Set the address and port of the new database server
   - Set the user name and password
     - The final result should look like:
```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETERAI
```
9. **Start** the ERA Server/Proxy and verify that the ERA Server/Proxy service is running correctly.

3.3 ISO image

An ISO image file is one of the formats you can download (All-in-one Installers category) ESET Remote Administrator installers in. The ISO image contains the following:

- ERA Installer package
- Separate installers for each component

The ISO image is useful when you want to keep all ESET Remote Administrator installers in one place. It also eliminates the need to download the installers from the ESET website every time you need to run the installation. The ISO image is also useful to have when you want to install ESET Remote Administrator on a virtual machine.

3.4 Virtual appliance

ERA Server can be deployed in a VMware or Microsoft Hyper-V environment. The ERA Virtual appliance comes as an OVA (Open Virtualization Appliance) file. The OVA file is a template that contains a functional CentOS 6.5 operating system. You can deploy either ERA Server, ERA Proxy or ERA MDM using the appropriate template. When deploying an OVF template in VMware, follow the instructions from the Setup wizard that to specify the password for your ERA administrator account and configure the virtual machine before deployment. Once the appliance is deployed, the virtual machine is a complete environment with ESET Remote Administrator ready to be used.

ERA Virtual appliances are vmx-07 virtual hardware family type, and are supported by the following VMware Hypervisors:

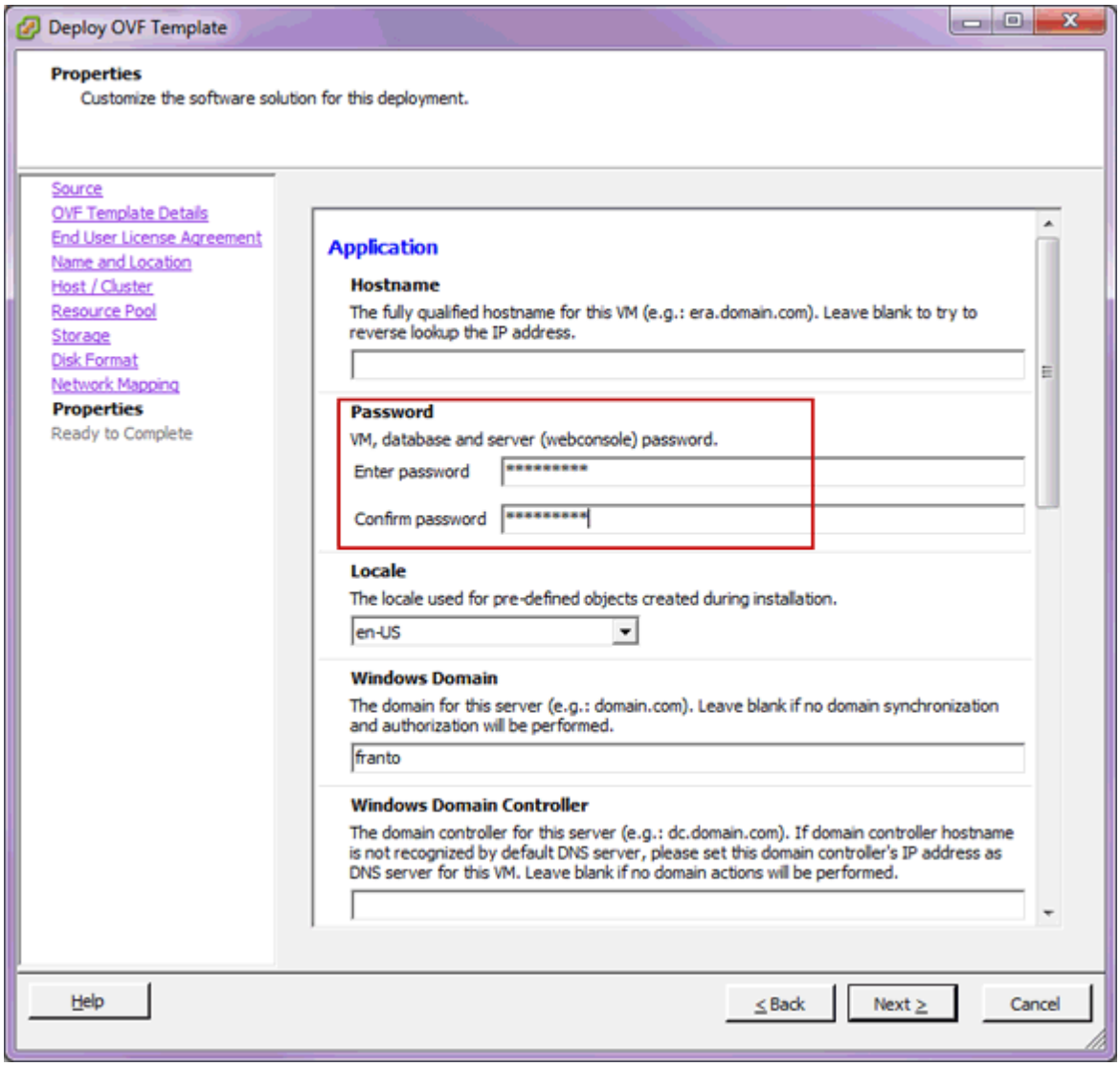
- ESXi 5.0 and newer
- Workstation 6.5 and newer

It is possible to use VMware Player or Oracle VirtualBox on a desktop operating system and deploy the virtual appliance using this configuration. This lets you run ESET Remote Administrator on a non-server OS with no need for enterprise-level ESXi. This applies to the `ERA_Server.ova` file only.

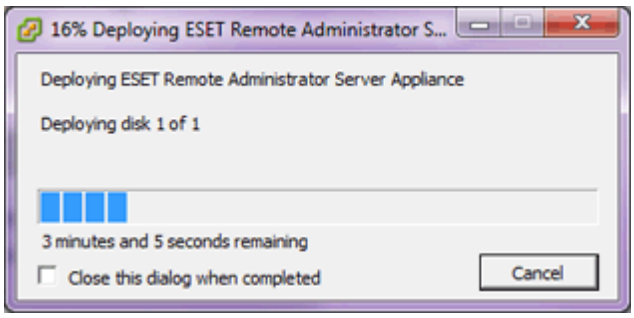
Deploying an OVF Template in vSphere Client

1. Connect to vCenter Server using vSphere Client (do not connect directly to ESXi server).
2. Click **File** in the top menu bar and select **Deploy OVF Template**.
3. Click **Browse**, navigate to the OVA file you downloaded from the ESET website and then click **Open**. Depending on which component you want to deploy, use the `ERA_Server.ova`, `ERA_Proxy.ova` or `ERA_MDM.ova` file.
4. Click **Next** in the OVF Template Details window.
5. Read and accept the End User License Agreement (EULA).
6. Follow the instructions on screen to complete installation and specify the following information about your virtual client:
   - Name and Location
   - Host/Cluster
   - Resource Pool
   - Storage
   - Disk Format
   - Network Mapping
6. In the **Properties** page, specify a **Hostname** (this will be your ERA Server or ERA Proxy hostname) and **Password**. This password is important, as it will be used in all ERA components—ERA database, ERA Server and ERA Web Console—as well as for access to your ERA Virtual Machine (CentOS).

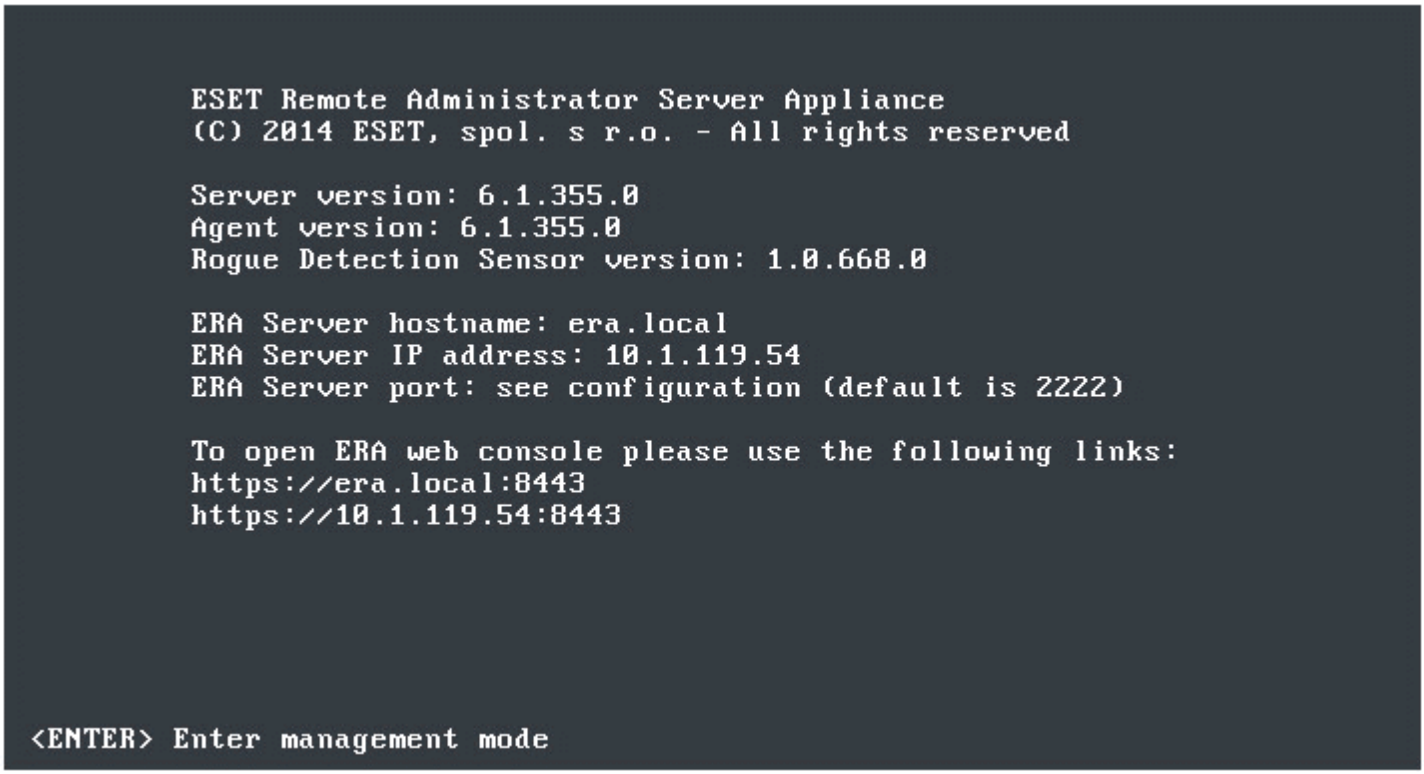
7. The rest of the fields are optional, you can specify your **Windows Domain** details which are useful for Static Group Synchronization. You can also set **Networking Properties**.


Deploy OVF Template
Properties
Customize the software solution for this deployment.
Source
OVF Template Details
End User License Agreement
Name and Location
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Application
Hostname
The fully qualified hostname for this VM (e.g.: era.domain.com). Leave blank to try to reverse lookup the IP address.
Password
VM, database and server (webconsole) password.
Enter password
Confirm password
Locale
The locale used for pre-defined objects created during installation.
en-US
Windows Domain
The domain for this server (e.g.: domain.com). Leave blank if no domain synchronization and authorization will be performed.
franto
Windows Domain Controller
The domain controller for this server (e.g.: dc.domain.com). If domain controller hostname is not recognized by default DNS server, please set this domain controller's IP address as DNS server for this VM. Leave blank if no domain actions will be performed.
Help
< Back
Next >
Cancel

8. Click **Next**, review the deployment summary and click **Finish**. The process will automatically create a virtual machine with the settings you specified. Once the VM is successfully created, you can power it on.


16% Deploying ESET Remote Administrator S...
Deploying ESET Remote Administrator Server Appliance
Deploying disk 1 of 1
3 minutes and 5 seconds remaining
Close this dialog when completed
Cancel

9. When you open your VMware console after deploying ERA, you will see the following information with your ERA Web Console URL in the format *https:///[IP address]:8443*. Type the displayed URL into your web browser to Log into your ERA Web Console (use the password that you specified in step 6).


ESET Remote Administrator Server Appliance
(C) 2014 ESET, spol. s r.o. - All rights reserved
Server version: 6.1.355.0
Agent version: 6.1.355.0
Rogue Detection Sensor version: 1.0.668.0
ERA Server hostname: era.local
ERA Server IP address: 10.1.119.54
ERA Server port: see configuration (default is 2222)
To open ERA web console please use the following links:
https://era.local:8443
https://10.1.119.54:8443
<ENTER> Enter management mode

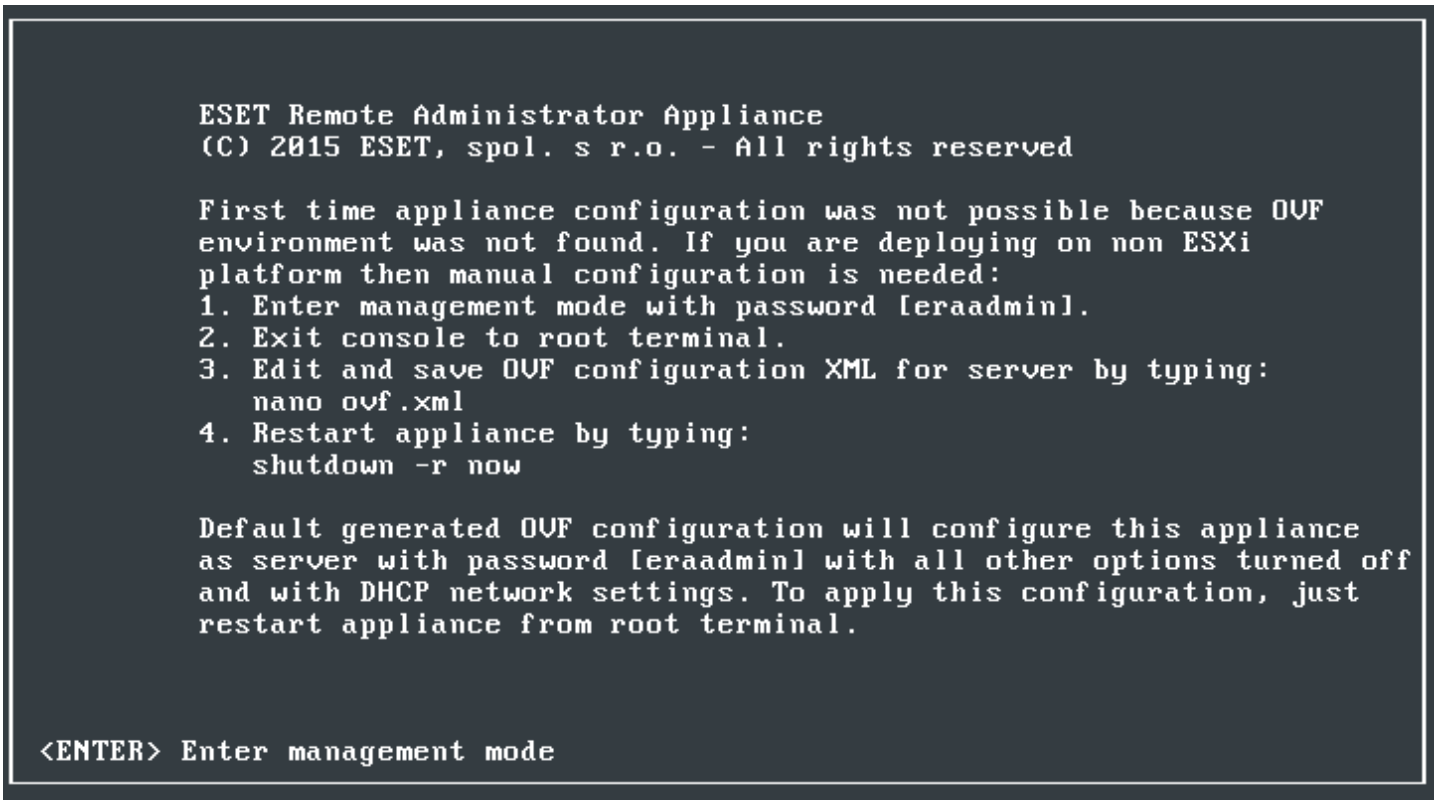
NOTE: We highly recommend that you configure vCenter Roles and Permissions in such a way that VMware users won't be able to access the ERA virtual machine. This will prevent users tampering with the ERA VM. There is no need for ERA users to access the VM. To manage access to ESET Remote Administrator itself, use Access Rights within the ERA Web Console.

3.4.1 VMware Player

Deploying an OVF Template in VMware Player

We recommend that you use the latest version of VMware Player.

1. Select **File** > **Open a Virtual Machine**.
2. Navigate to the OVA file (`ERA_Server.ova`) that you downloaded from the ESET website. Click **Open**.
3. Provide a name and local store path for the new virtual machine and click **Import.**
4. Read and accept the End User License Agreement (EULA) if you agree with it.
5. Once the appliance is deployed, power it on. The following information will be displayed:


ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved
First time appliance configuration was not possible because OVF environment was not found. If you are deploying on non ESXi platform then manual configuration is needed:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
nano ovf.xml
4. Restart appliance by typing:
shutdown -r now
Default generated OVF configuration will configure this appliance as server with password [eraadmin] with all other options turned off and with DHCP network settings. To apply this configuration, just restart appliance from root terminal.
<ENTER> Enter management mode

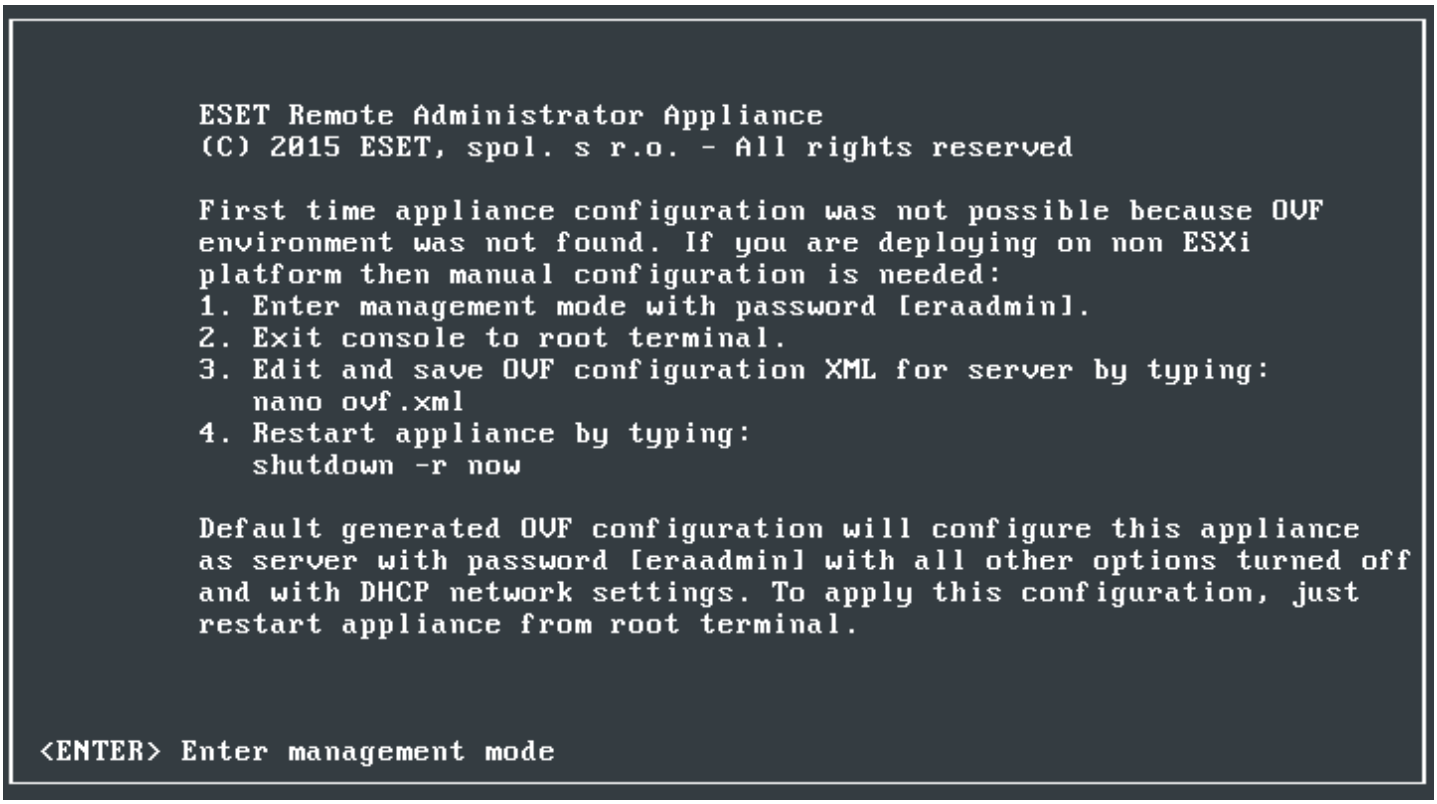
6. You must modify the `ovf.xml` configuration file to include your database connection details, etc. To do so, follow the instructions on screen.

3.4.2 Oracle VirtualBox

Deploying an OVA file in VirtualBox

We recommend that you use the latest version of VirtualBox.

1. Click **File** and select **Import Appliance...**
2. Click **Browse** and navigate to the OVA file (`ERA_Server.ova`) which you downloaded from the ESET website and then click **Open**. Click **Next**.
3. Review your appliance settings and click **Import**.
4. Read and accept the End User License Agreement (EULA) if you agree with it.
5. Once the appliance is deployed, power it on. The following information will be displayed:


ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved
First time appliance configuration was not possible because OVF environment was not found. If you are deploying on non ESXi platform then manual configuration is needed:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
nano ovf.xml
4. Restart appliance by typing:
shutdown -r now
Default generated OVF configuration will configure this appliance as server with password [eraadmin] with all other options turned off and with DHCP network settings. To apply this configuration, just restart appliance from root terminal.
<ENTER> Enter management mode

6. You must modify the `ovf.xml` configuration file to include your database connection details, etc. To do so, follow the instructions on screen.

3.4.3 Microsoft Hyper-V

Deploying an OVA file in Microsoft Hyper-V

1. Extract the files (which you downloaded from the ESET website) from the virtual appliance file (`ERA_Server.ova`) using a utility such as Tar or 7-Zip. You'll see a number of extracted files including the `.vmdk` file (for example `ERA_Server-disk1.vmdk`).
2. Download and install Microsoft Virtual Machine Converter 3.0 http://www.microsoft.com/en-us/download/details.aspx?id=42497.
3. Make sure that you have Windows PowerShell 3.0 (or later) available on your system, especially on Windows 7. To do so, follow the instructions below:

a. open a Windows Command Prompt (**cmd.exe**).
b. type `powershell` into the command prompt and press **Enter**.
c. In PowerShell, type `$PSVersionTable` and press **Enter**.
d. If **PSVersion 3.0** (or later) is displayed, go to step 5. If not, download and install Windows Management Framework 3.0 http://www.microsoft.com/en-us/download/details.aspx?id=34595.
e. Repeat steps a-c to verify that Powershell 3.0 or later is installed and then skip to step 5.

4. Run PowerShell and execute the commands in the following steps.

5. Run the Import module command:
```
import-Module 'C:\Program Files\Microsoft Virtual Machine Converter\MvmcCmdlet.psd1'
```

6. To confirm that the import was successful, review the modules imported using the following command:
```
get-command -Module mvmccmdlet
```

7. Convert the `.vmdk` disk you extracted in step 1. (`ERA_Server-disk1.vmdk` if you're deploying ERA Server):

   a. In Windows 7, you must use the **VHD format**:
```
ConvertTo-MvmcVirtualHardDisk -SourceLiteralPath <path>\ERA_Server-disk1.vmdk -
DestinationLiteralPath <output-dir> -VhdType DynamicHardDisk -VhdFormat Vhd
```

   b. In Windows 8 and later, you can use the **VHDX format**:
```
ConvertTo-MvmcVirtualHardDisk -SourceLiteralPath <path>\ERA_Server-disk1.vmdk -
DestinationLiteralPath <output-dir> -VhdType DynamicHardDisk -VhdFormat Vhdx
```

8. Connect to Hyper-V.

9. Create a new virtual machine (Generation 1) with at least 4 Cores and 4 GB of RAM. This virtual machine will use the disk you converted in step 7.

3.5 Failover Cluster - Windows

Below are the high-level steps required to install ESET Remote Administrator in a Failover Cluster environment:

1. Create a Failover Cluster. It should have a shared disk, IP address and a cluster name.

   a. Instructions to create a failover cluster in Windows Server 2012

   b. Instructions to create a failover cluster in Windows Server 2008

2. Install ERA Server and ERA Agent on the active node. Choose the shared disk as application data storage.

3. Change the active node, and repeat step 2.

4. In the cluster configuration manager create 2 cluster services: ERA Agent and ERA Server.

5. Set the appropriate dependencies: the services should start after the resources from step 1 are initialized. Also, ERA Agent should be dependent on ERA Server.

6. The Database and Web Server are not supported on a cluster.

NOTE: It is not possible to install ERA Server on a Failover Cluster via ERA Installer. To install ESET Remote Administrator on a Failover Cluster perform a component installation.

3.6 Failover Cluster - Linux

The following refers to ESET Remote Administrator installation and configuration on a Red Hat high-availability cluster.

- Linux Cluster Support
- Prerequisites
- Scope
- Installation steps

Linux Cluster Support

ESET Remote Administrator Server or ERA Proxy components can be installed on **Red Hat Linux 6** cluster and higher. Failover Cluster is only supported in active/passive mode with the cluster manager **rgmanager**.

Prerequisites

- Active/passive cluster must be installed and configured. Only one node can be active at a time, other nodes must be on standby. Load balancing is not supported.
- Shared storage - iSCSI SAN, NFS and other solutions are supported (any technology or protocol which provides block based or file based access to shared storage, and makes the shared devices appear like locally attached devices to the operating system). Shared storage must be accessible from each active node in the cluster, and the shared file system must be properly initialized (for example, using the EXT3 or EXT4 file system).
- The following HA add-ons are required for system management:
    - rgmanager
    - Conga
- **rgmanager** is the traditional Red Hat HA cluster stack. It is a mandatory component.
- The **Conga** GUI is optional. The Failover Cluster can be managed without it, however we recommend that you install it for best performance. In this guide we assume that it is installed.
- **Fencing** must be properly configured in order to prevent data corruption. The cluster administrator must configure fencing if it is not already configured.

If you do not already have a cluster running, you can use the following guide to set up a high-availability Failover Cluster (active/passive) on Red Hat: Red Hat Enterprise Linux 6 Cluster Administration.

Scope

ESET Remote Administrator components that can be installed on a **Red Hat Linux** HA cluster:

- ERA Server with ERA Agent
- ERA Proxy with ERA Agent

NOTE: ERA Agent must be installed, otherwise the ERA cluster service will not run.

NOTE: Installation of the ERA Database or ERA Web Console on a cluster is not supported.

The following installation example is for a 2-node cluster. However, you can install ESET Remote Administrator on a multi-node cluster using this example as a reference only. The cluster nodes in this example are named **node1** and **node2**.

Installation steps

1. Install ERA Server or ERA Proxy and then ERA Agent on node1. During ERA Agent installation, when using the `--hostname=` command, you have the option to specify `localhost` (do not use IP address or actual hostname of that particular node). Alternatively, you can specify the external IP address or host name of the cluster's interface.

- Please note that the hostname in the Server or Proxy certificate must contain the external IP (or hostname) of the cluster's interface (not local IP or hostname of the node).
- During ERA Agent installation, when using the --hostname= command, you have the following options:
  - You can specify the external IP address or host name of the cluster's interface.
  - Alternatively you can specify localhost (not the IP address or actual hostname of that particular node). In this case the ERA Server or ERA Proxy certificate hostname must contain in addition localhost.

2. Stop and disable the ERA Agent and ERA Server (or ERA Proxy) Linux services using the following commands:

```
chkconfig eraagent off
chkconfig eraserver off
service eraagent stop
service eraserver stop
```

3. Mount shared storage to node1. In this example, the shared storage is mounted to **/usr/share/erag2cluster**.

4. In **/usr/share/erag2cluster**, create the following directories:

   /usr/share/erag2cluster/etc/opt
   /usr/share/erag2cluster/opt
   /usr/share/erag2cluster/var/log
   /usr/share/erag2cluster/var/opt

5. Move recursively the following directories to the destinations shown below (source > destination):

Move folder:	Move to:
/etc/opt/eset	/usr/share/erag2cluster/etc/opt/
/opt/eset	/usr/share/erag2cluster/opt/
/var/log/eset	/usr/share/erag2cluster/var/log/
/var/opt/eset	/usr/share/erag2cluster/var/opt/

6. Create symbolic links:

```
ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset
```

7. Unmount the shared storage from node1, mount it to the same directory that you mounted to on node1 (**/usr/share/erag2cluster**) on node2.

8. On node2, create the following symbolic links:

```
ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset
```

9. Copy the script `eracluster_server` (`eracluster_proxy`) to **/usr/share/cluster**.

   The `eracluster_server` (`eracluster_proxy`) scripts are located in the setup directory of ERA Server or ERA Proxy.

The next steps are performed in Conga Cluster Administration GUI:

10. Create a service group, for example EraService.

The ESET Remote Administrator cluster service requires three resources: IP address, file system and script.

11. Create the necessary service resources.

    Add an IP address, file system and Script resources.
    The file system resource should point to the shared storage.
    The mount point of the file system resource should be set to **/usr/share/erag2cluster**.
    The "Full Path to Script File" parameter of the Script resource should be set to **/usr/share/cluster/eracluster_server** (or **/usr/share/cluster/eracluster_proxy**).

12. Add the above resources to the EraService group.

3.7 Component installation on Windows

In most installation scenarios, you need to install different ESET Remote Administrator components on different machines to accommodate different network architectures, meet performance requirements, or for other reasons. Installation packages for individual components are available for this type of install.

Core components

- ERA Server
- ERA Web Console
- ERA Agent (must be installed on client computers, optional on ERA Server)

Optional components

- ERA Proxy
- RD Sensor
- Mobile Device Connector
- Apache HTTP Proxy

If you need to upgrade ESET Remote Administrator to the latest version (6.x) see our Knowledgebase article.

3.7.1 Server installation - Windows

To install the ERA Server component on Windows, follow these steps:

1. Make sure all prerequisites are met.
2. Run the ERA Server installer and accept the EULA if you agree with it.

NOTE: If you are installing ERA Server on a Failover Cluster, select the check box next to **This is cluster installation**. Otherwise, leave this check box empty.

3. If installing on a Failover Cluster, specify the **Custom application data path** to point to the shared storage for the cluster. The data must be stored at one location that is accessible by all nodes within the cluster.
4. Enter a valid ERA License Key or choose **Activate Later**.
5. Select a **Service user account**. This account will be used to run the ESET Remote Administrator Server Service. The following options are available:
    - Network service account
    - User specified: DOMAIN/USERNAME
4. Connect to a Database. All data is stored here (ERA Web Console password, client computer logs, etc.):
    - **Database**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication
    - **ODBC Driver**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server
    - **Database name**: you can leave the predefined name or change it if required
    - **Hostname**: hostname or the IP address of your database server
    - **Port:** used for connection to the database server
    - Database admin account **Username**/**Password**

NOTE: ERA Server stores large data blobs in the database, therefore it is necessary to configure MySQL to accept large packets for ERA to run properly. For details on how to configure do this see our FAQ.

This step will verify your connection to the database. If the connection is ok, you can proceed to the next step.

5. Select a user for ESET Remote Administrator that has access to the database. You can use an existing user, or setup can create one for you.
6. Enter a password for **Web Console** access.

7. ESET Remote Administrator uses certificates for client-server communication. You can either select your own certificates, or the **Server** can create new certificates for you.
8. Enter the password for the **Certification authority**. Be sure to remember this password.
9. A new certificate server will be created, select a password for it as well.
10. In the next step, select a password for the **Agent** certificate.

Setup can perform an initial Static Group Synchronization task. Select the method (**Do not synchronize**, **Sync with Windows Network**, **Sync with Active Directory**) and click **Next**.

Confirm or change the installation folder for the server and click **Next**.

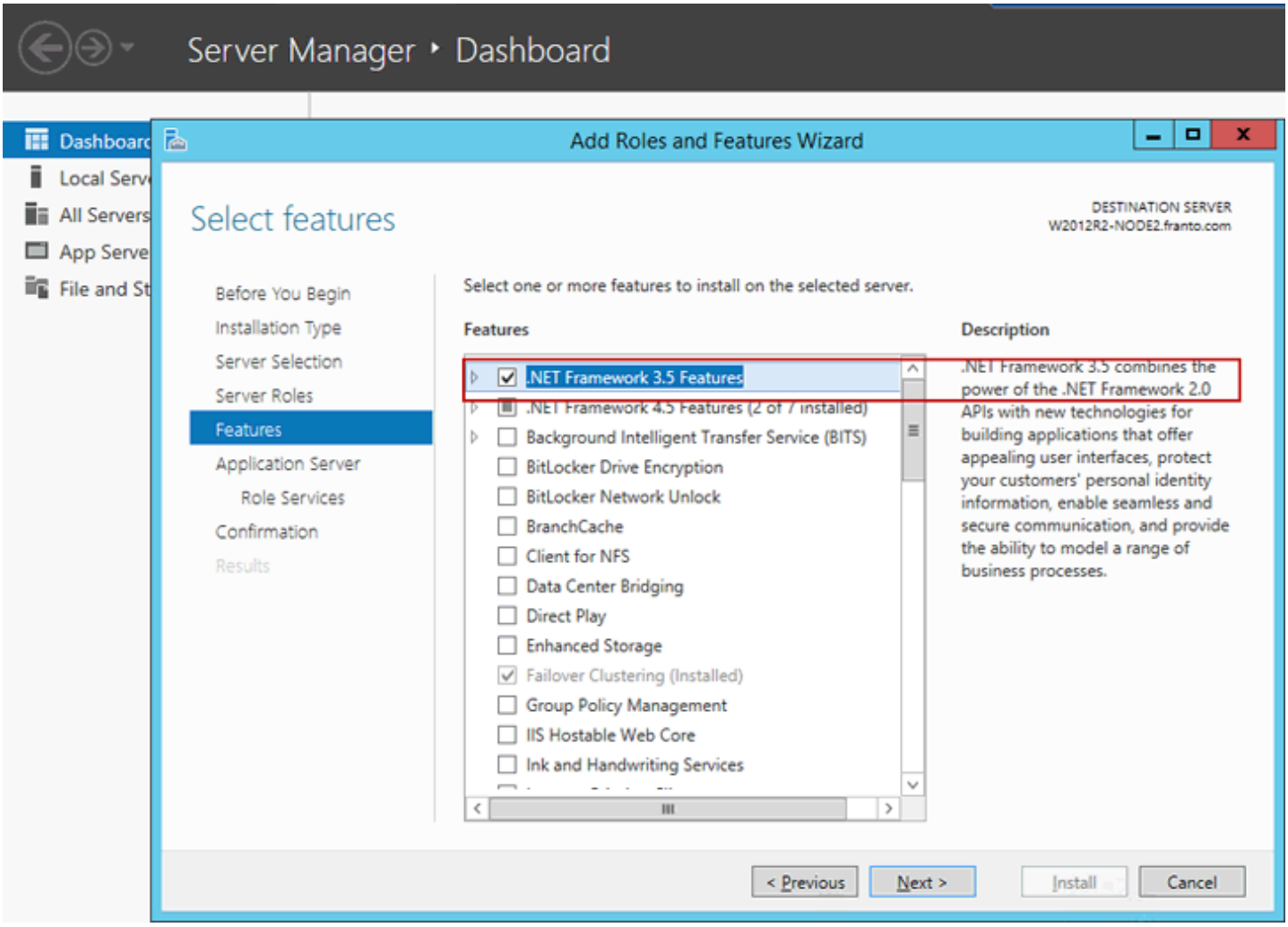
Click **Install** to install the server.

NOTE: Once you have completed the installation of the ERA Server, you can also install ERA Agent on the same machine (optional). This way you'll be able to manage the server itself the same way as you would mange a client computer.

3.7.1.1 Server prerequisites - Windows

The following prerequisites must be met to install ERA Server on Windows:

- You must have a valid license.
- Required ports must be open and available—see the complete list of ports here.
- Database server (Microsoft SQL Server or MySQL) installed and running, see database requirements for details. If you do not have an existing database server, we recommend you to review the SQL Server configuration details in to have SQL properly configured for use with ESET Remote Administrator.
- Java Runtime Environment (JRE) must be installed (you can download it from http://java.com/en/download/), always use the latest officially released version of Java.
- Microsoft .NET Framework 3.5 must be installed, if you are running Windows Server 2008 or 2012 you can install it using the **Roles and Features Wizard** (as shown below), if you are using Windows Server 2003, you can download .NET 3.5 here: http://www.microsoft.com/en-us/download/details.aspx?id=21


Server Manager ‣ Dashboard
Add Roles and Features Wizard
Select features
DESTINATION SERVER
W2012R2-NODE2.franto.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Application Server
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
Description
.NET Framework 3.5 Features
.NET Framework 4.5 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering (Installed)
Group Policy Management
IIS Hostable Web Core
Ink and Handwriting Services
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

NOTE: If you choose to install Microsoft SQL Server Express during ESET Remote Administrator installation, you will not be able to install it on a Domain Controller. This is likely to happen if you are using Microsoft SBS. If you use Microsoft SBS, we recommend that you install ESET Remote Administrator on a different server or do not select the SQL Server Express component during the installation (this requires you to use your an existing SQL Server or MySQL to run ERA database). For instructions to install ERA Server on a Domain Controller, see our Knowledgebase article.

NOTE: ERA Server stores large data blobs in the database, therefore it is necessary to configure MySQL to accept large packets for ERA to run properly. For instructions to make this change see the FAQ.

3.7.2 Microsoft SQL Server - Windows

One of the prerequisites for the installation of ERA Server is to have Microsoft SQL Server installed and configured for use with ESET Remote Administrator. The following requirements must be met:

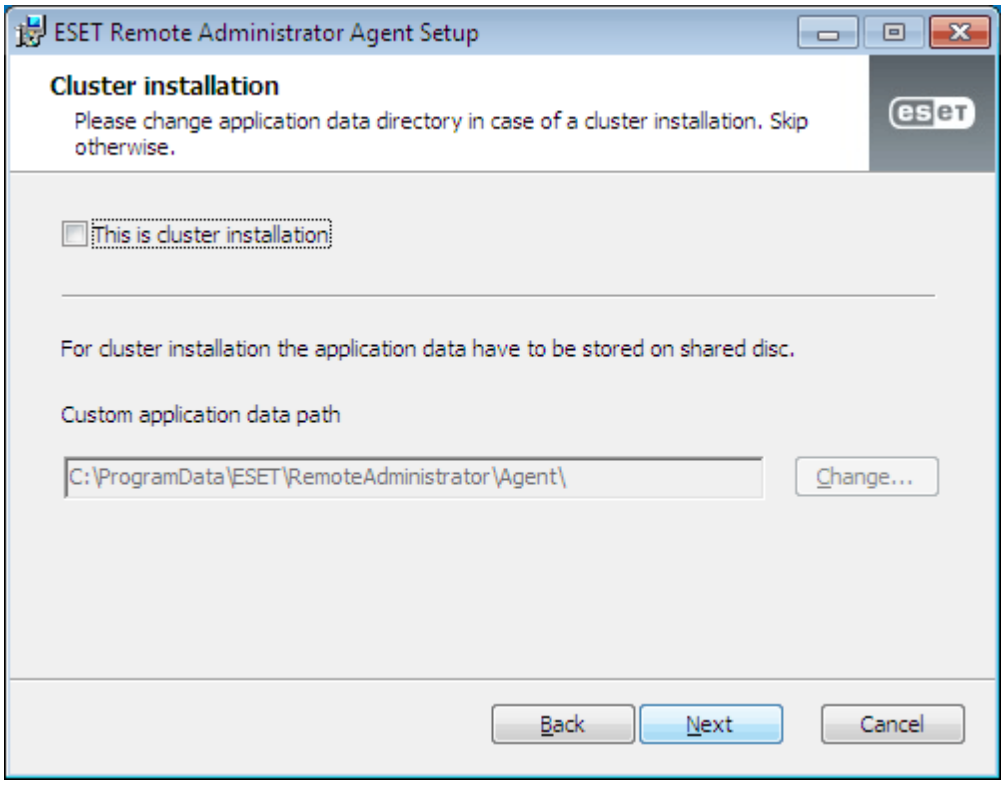
- Install Microsoft SQL Server 2008 R2 or later, alternatively you can install Microsoft SQL Server 2008 R2 Express or later. Choose **Mixed mode** authentication during installation.
- If you have Microsoft SQL Server already installed, set authentication to **Mixed mode (SQL Server authentication and Windows authentication)**. To do so, follow the instructions in this KnowledgeBase article.
- Allow TCP/IP connections to the SQL Server. To do so, follow instructions in this Knowledgebase article from part **II. Allow TCP/IP connections to the SQL database**.

3.7.3 Agent installation - Windows

To install the ERA Agent component on Windows, follow these steps:

1. Run the ERA Agent installer and accept the EULA if you agree with it.

NOTE: If you are installing ERA Agent on a Failover Cluster, select the check box next to **This is cluster installation**. Otherwise, leave this check box empty.



2. If installing on a Failover Cluster, specify the **Custom application data path** to point to the shared storage of the cluster. The data must be stored in one location that is accessible for all nodes within the cluster.
3. Enter the **Server host** (name or IP address of your ERA Server) and **Server port** (default port is 2222, if you are using different port, then replace the default port with your custom port number).

Select one of the following installation options and follow the steps from the appropriate section below:

- **Server assisted installation** - you'll need to provide ERA Web Console administrator credentials (installer will download the required certificates automatically).
- **Offline installation** - you'll need to provide an **Agent certificate** which can be exported from ESET Remote Administrator. Alternatively, you can use your custom certificate.

Server assisted installation:

4. Enter **Server host** - name or IP address of your ERA Server and **Web Console port** (leave default port 2223 if you are not using custom port). Also, provide Web Console administrator account credentials - **Username**/**Password**.
5. Click **Yes** when asked if you want to accept the certificate.
6. Choose **Do not create computer** or **Choose custom static group**. If you click **Choose custom static group** you'll be able to select from a list of existing Static groups in ERA. The computer will be added to the group you've selected.
7. Specify a destination folder for ERA Agent (we recommend using the default location), click **Next** and then click **Install**.

Offline installation:

4. Click **Browse** and navigate to the location of your Peer certificate (this is the Agent certificate you exported from ERA). Leave the **Certificate password** text field blank as this certificate does not require a password. You do not need to browse for a **Certification authority** - leave this field empty.

NOTE: If you are using a custom certificate with ERA (instead of the default ones that was automatically generated during ESET Remote Administrator installation), use your custom certificates accordingly.

5. Click **Next** to install to the default folder or click **Change** to choose another (we recommend using the default location).

3.7.4 Web Console installation - Windows

To install the ERA Web Console component on Windows, follow the steps below:

1. Make sure the following prerequisites are met:
   - Java—always use the latest officially released version of Java (ERA Web Console requires at least Java version 7, but we strongly recommend that you use the latest version).
   - Apache Tomcat (version 6 or later).
   - Web Console file (*era.war*) saved to your local hard drive.
2. Copy *era.war* to the Tomcat web applications folder (on most operating systems - *C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\).*
3. Restart the *Apache Tomcat* service.
4. Open https://localhost/era/ in your browser on localhost—a login screen will be displayed.

3.7.4.1 Supported Web browsers

Web Browser	Version
Mozilla Firefox	20+
Internet Explorer	10+
Chrome	23+
Safari	6+
Opera	12+

3.7.5 Proxy installation - Windows

To install the ERA Proxy server component on Windows, follow these steps:

1. Make sure all prerequisites are met.

NOTE: In case you are installing ERA Proxy server on a Failover Cluster, select check box **This is cluster installation**. Otherwise, leave this check box empty.

2. If installing on a Failover Cluster, specify the **Custom application data path** to point to a shared storage of the cluster. The data must be stored at one location that is accessible by all nodes within the cluster.
3. Select a Service user account. This account will be used to run the ESET Remote Administrator Server Service. The following options are available:

   a. Network service account
   b. Custom account: DOMAIN/USERNAME

4. Connect to a Database. All data is stored here, from the ERA Web Console password to client computer logs.

   a. Database: MySQL/MS SQL
   b. ODBC Driver: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 ANSI/ DriverSQL Server
   c. Hostname of the database server
   d. The port used for connection with the Server
   e. Database name
   f. DB Admin login/password
   g. ERA Database user login/password

This step will verify your connection to the database. If the connection is ok, you can proceed to the **next** step. An error message will be displayed if a connection cannot be established.

4. Select a proxy communication port. By default port 2222 is used.
5. Configure the proxy connection to ESET Remote Administrator. Enter a **Server host** (hostname/ip address of the Server) and the **Server port** (2222).
6. Select a peer certificate and a password for this certificate. Optionally, also add a certificate authority. This is only needed for unsigned certificates.
7. Select a folder where the **Proxy** will be installed or leave the pre-defined folder selected.
8. Click **Install**. The **Proxy** will be installed on your computer.

NOTE: Server assisted installation is not supported when installing ERA Proxy.

3.7.5.1 Proxy prerequisites - Windows

The following prerequisites must be met in order to install ERA Proxy server component on Windows:

- **ERA Server** and the **ERA Web Console** installed (on a Server computer).
- **Proxy Certificate** created and downloaded to your local drive.
- **Certificate Authority** prepared on your local drive.
- A valid license.
- A database server already installed and configured.
- An ODBC Driver for the connection to the database server (MySQL / MS SQL) installed on the computer.
- Agent must be installed on a local computer to fully support all program features.

3.7.6 RD Sensor installation - Windows

To install the RD Sensor component on Windows, follow these steps:

1. Make sure all prerequisites are met.
2. Double-click the RD Sensor installer file to begin installation.
3. Select the location where RD Sensor will be installed and click **Next** > **Install**.

3.7.6.1 RD Sensor prerequisites - Windows

The following prerequisites must be met in order to install the RD Sensor component on Windows:

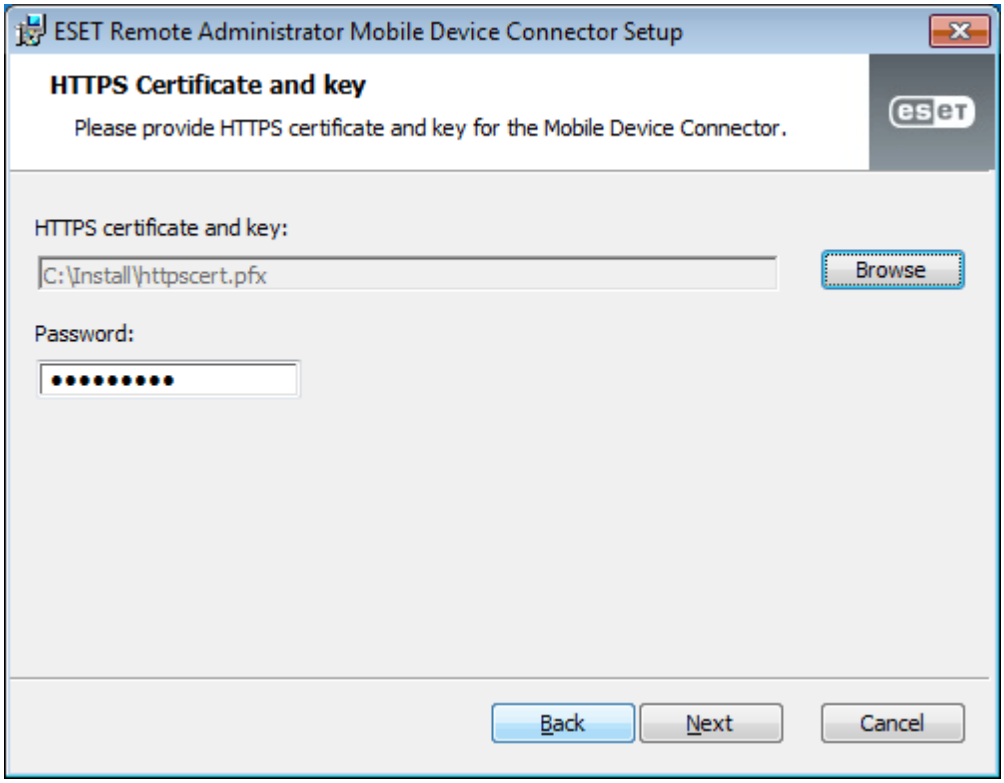
- WinPcap - use the latest WinPcap version (at least 4.1.0)
- Network should be properly configured (appropriate ports open, incoming communication not being blocked by a firewall, etc.)
- ERA Server reachable
- ERA Agent must be installed on the local computer to fully support all program features
- Rogue Detection Sensor log file can be found here: *C:\ProgramData\ESET\Rouge Detection Sensor\Logs\trace.log*

3.7.7 Mobile Device Connector installation - Windows

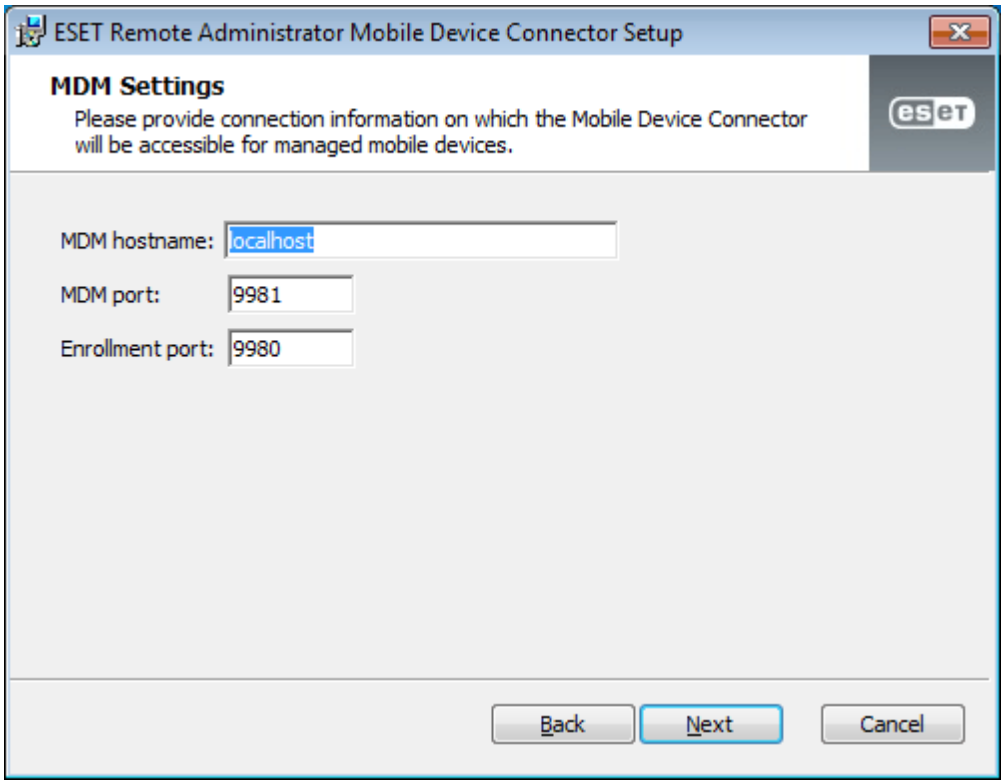
You can install the Mobile Device Connector component on a different server than the one on which your ERA Server is running. For example, if you want to make Mobile Device Connector accessible from the internet so that the user's mobile devices can be managed at all times regardless of their location.

Follow the steps below to install Mobile Device Connector on Windows:

1. Make sure all prerequisites are met.
2. Run the Mobile Device Connector installer and accept the EULA if you agree with it.
3. Click **Browse**, navigate to the location of your SSL certificate for communication via HTTPS, type in the password for this certificate:



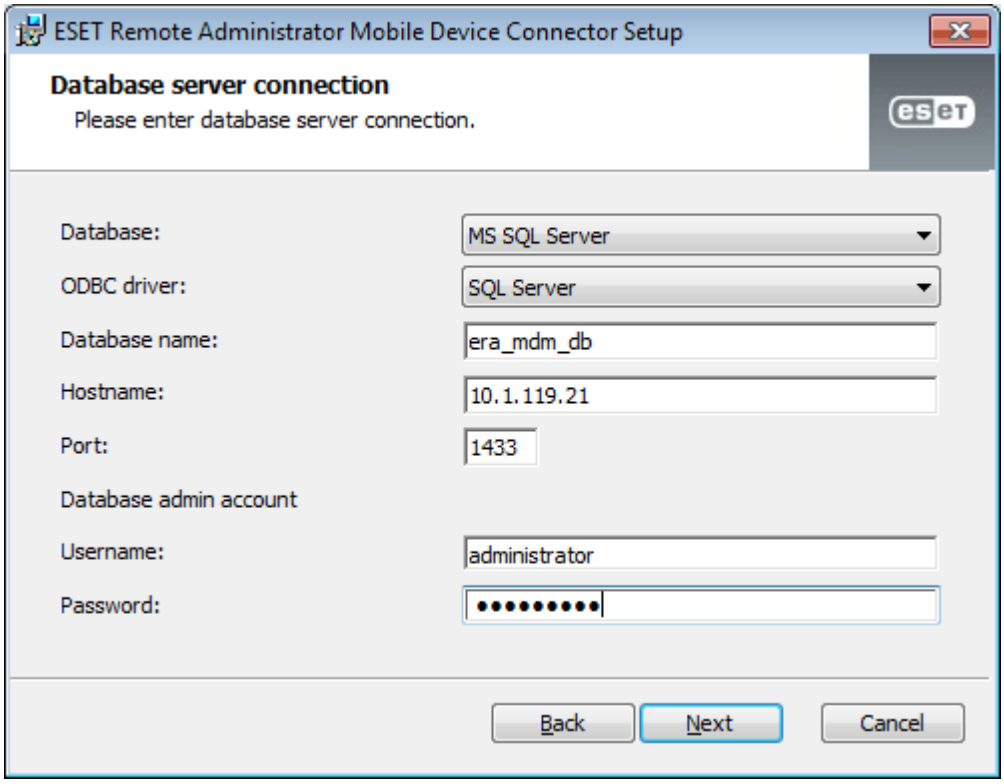
4. We recommend that you use the default hostname and ports (9981 and 9980), but you can specify your own ports if required. Make sure that devices are able to connect via these two ports to the server where you're installing Mobile Device Connector. Change your firewall settings (if applicable) to make this possible.



5. Installer needs to create new database which will be used by Mobile Device Connector, therefore provide connection details:

- **Database**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication
- **ODBC Driver**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server
- **Database name**: you can leave predefined name or change it if required
- **Hostname**: hostname or the IP address of your database server
- **Port:** used for connection to the database server
- Database admin account **Username**/**Password**

NOTE: We recommend using the same database server you're using for ERA database, but it can be different DB server if required. When you click Next button, Mobile Device Connector installer will create its database.



6. Specify user for newly created Mobile Device Connector database. You can **Create new user** or **Use existing database user**. Type in the password for the database user.
7. Enter **Server host** (name or IP address of your ERA Server) and **Server port** (default port is 2222, if you are using different port, then replace the default port with your custom port number).

Now you have two options how to continue with the installation:

- **Server assisted installation** - you'll need to provide ERA Web Console administrator credentials (installer will download required certificates automatically).
- **Offline installation** - you'll need to provide **Agent certificate** which can be exported from ESET Remote Administrator. Alternatively, you can use your custom certificate.

These steps apply if choose **Server assisted installation**:

8. Enter **Server host** - name or IP address of your ERA Server and **Web Console port** (leave default port 2223 if you are not using custom port). Also, provide Web Console administrator account credentials - **Username**/**Password**.
9. When asked to **Accept Certificate**, click **Yes**.
10. Specify destination folder for Mobile Device Connector (we recommend using default), click **Next** and then **Install**.

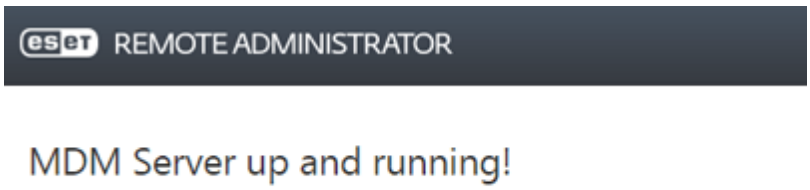
These steps apply if choose **Offline installation**:

8. Click **Browse** and navigate to the location with Peer certificate (this is the Agent certificate you've exported from ERA). Leave the **Certificate password** text field blank as this certificate does not require password.

NOTE: In case you are using your custom certificates with ERA (instead of the default ones that were automatically generated during ESET Remote Administrator installation), then use your custom certificates accordingly.

9. Click **Next** to install to the default folder or click **Change...** to choose another (we recommend using default).

After the installation is complete, check if the Mobile Device Connector is running correctly by opening https://*your-mdm-hostname*:*enrollment-port* (for example https://eramdm:9980) in your web browser. If the installation was successful, you'll see following message:

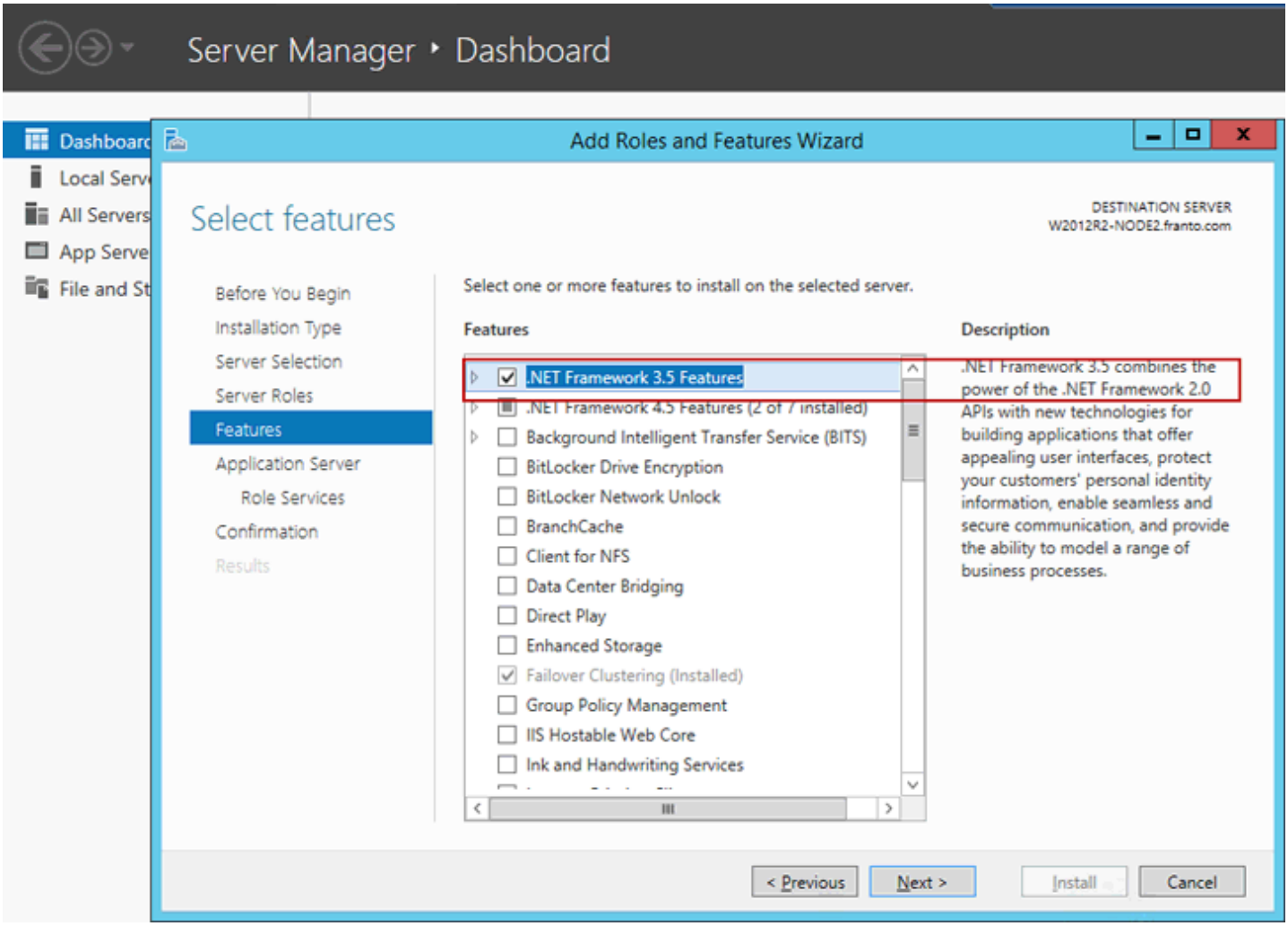


You can also use this URL to check the availability of the Mobile Device Connector server from the internet (if configured in such a way) by visiting it from a mobile device for example. If you are unable to reach the page, you might want to check your firewall and other configuration of your network infrastructure.

3.7.7.1 Mobile Device Connector prerequisites - Windows

The following prerequisites must be met in order to install Mobile Device Connector on Windows:

- Ports open and available - see the complete list of ports here.
- Firewall settings - if installing Mobile Device Connector on non-server OS such as Windows 7 (for evaluation purpose only), make sure to allow communication ports by creating firewall rules for:
  C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9980
  C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9981
  C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP port 2222
  NOTE: Actual paths to `.exe` files may vary depending on where each of the ERA components is installed on your client OS system.
- Java Runtime Environment (JRE) must be installed (you can download it from http://java.com/en/download/), always use the latest officially released version of Java.
- Microsoft .NET Framework 3.5 must be installed, if you are running Windows Server 2008 or 2012 you can install it using the **Roles and Features Wizard** (as shown below), if you are using Windows Server 2003, you can download .NET 3.5 here: http://www.microsoft.com/en-us/download/details.aspx?id=21


Server Manager • Dashboard
Add Roles and Features Wizard
Select features
DESTINATION SERVER
W2012R2-NODE2.franto.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Application Server
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
Description
.NET Framework 3.5 Features
.NET Framework 4.5 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering (Installed)
Group Policy Management
IIS Hostable Web Core
Ink and Handwriting Services
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

NOTE: If you choose to install Microsoft SQL Server Express during ESET Remote Administrator installation, you will not be able to install it on a Domain Controller. This is likely to happen if you are using Microsoft SBS. If you use Microsoft SBS, we recommend that you install ESET Remote Administrator on a different server or do not select the SQL Server Express component during installation (this requires you to use your existing SQL Server or MySQL to run the ERA database).

NOTE: ERA Server stores large data blobs in the database, therefore it is necessary to configure MySQL to accept large packets for ERA to run properly. For instructions to make this change this see the FAQ.

IMPORTANT: You'll need an **SSL certificate** in `.pfx` format for secure communication over HTTPS. We recommend that you use the certificate provided by CA. Self-signed certificates are not recommended because not all mobile devices let users to accept self-signed certificates. This isn't an issue with CA signed certificates, because they are trusted and do not require acceptance by the user.

IMPORTANT: In the case of Offline installation , you'll also need an **Agent certificate** exported from ESET Remote Administrator. Alternatively, you can use your custom certificate with ERA.

3.7.8 Apache HTTP Proxy installation - Windows

Apache HTTP Proxy is a service that can be used in combination with ESET Remote Administrator 6 and later to distribute updates to client computers and installation packages to the ERA Agent. HTTP Proxy performs a similar role to the mirror server feature popular in ESET Remote Administrator 5 and earlier. Using HTTP Proxy offers the following benefits:

- Downloads new virus signature database updates and product component updates and then distributes them to clients on your network.
- Can cache ESET product installation packages.
- Minimized internet traffic on your network.

To install the Apache HTTP Proxy component on Windows, follow these steps:

1. Open ApacheHttp.zip and extract the files to *C:\Program Files\Apache HTTP Proxy*
2. Open an administrative command prompt and CD to *C:\Program Files\Apache HTTP Proxy\bin*
3. Execute the following command:

```
httpd.exe -k install -n ApacheHttpProxy
```

4. Using a text editor such as Notepad, open the httpd.conf file and add the following lines at the bottom of the file:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

5. Start the Apache HTTP Proxy service using the following command:

```
sc start ApacheHttpProxy
```

6. You can verify that the Apache HTTP Proxy service is running in the services.msc snap-in (look for **ApacheHttpProxy**). By default, the service is configured to start automatically.

Follow the steps below to configure a username and password for your Apache HTTP Proxy (recommended):

1. Verify the presence of the following modules in *Apache HTTP Proxy\conf\httpd.conf*:

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

2. Add the following lines to *Apache HTTP Proxy\conf\httpd.conf* under `<Proxy *>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

3. Use the `htpasswd` command to create a file named `password.file` in the folder *Apache HTTP Proxy\bin* (you'll be prompted for password):

```
htpasswd.exe -c ..\password.file username
```

4. Manually create the file `group.file` in the folder *Apache HTTP Proxy*\ with the following content:

```
usergroup:username
```

5. Test the connection to HTTP Proxy by accessing the following URL in your browser:

   http://localhost:3128/index.html

Use the htcacheclean tool to clean up the disk cache. This tool can run either manually or in daemon mode. Specify the limit as the total disk cache size limit. The value is expressed in bytes by default (or attaching B to the number). Add K for Kbytes or M for MBytes.

For more information please visit this Knowledgebase article or Apache Authentication and Authorization documentation.

3.8 Component installation on Linux

In most installation scenarios, you need to install different ESET Remote Administrator components on different machines to accommodate different network architectures, meet performance requirements, or for other reasons.

Core components

- ERA Server
- ERA Web Console
- ERA Agent

Optional components

- ERA Proxy
- RD Sensor
- Mobile Device Connector
- Apache HTTP Proxy

If you need to upgrade ESET Remote Administrator to the latest version (6.x) see our Knowledgebase article.

3.8.1 Server installation - Linux

Installation of the ERA Server component on Linux is performed using a command in the Terminal. Make sure all prerequisites are met. You can prepare an installation script and then execute it using *sudo*.

Example
(New lines are split by "\" for copying the whole command to Terminal)

```
sudo ./Server-Linux-i386.sh \
--skip-license \
--db-driver=MySQL \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=Admin123 \
--server-root-password=Admin123 \
--db-user-username=root \
--db-user-password=Admin123 \
--cert-hostname="10.1.179.46;Ubuntu64-bb;Ubuntu64-bb.BB.LOCAL"
```

The ERA Server and the `eraserver` service will be installed in the following location:
/opt/eset/RemoteAdministrator/Server

You can modify the following attributes:

Attribute	Description	Required
--uninstall	Uninstalls the product	-
--locale	The locale identifier (LCID) of installed server (default is "en_US"). See supported languages for possible options. **Note:** You can set a language for each ERA Web Console session.	Yes

Attribute	Description	Required
--skip-license	Installation will not ask user for license agreement confirmation	
--skip-cert	Skip generation of certificates (please use together with the --server-cert-path parameter)	
--license-key	ESET license key. This can be set later.	No
--product-guid	Global unique identifier of product. If not set, it will be generated.	No
--server-port	ESET Remote Administrator (ERA) server port (default 2222)	No
--console-port	ESET Remote Administrator console port (default 2223)	No
--server-root-password	Password for Web Console login of the user "Administrator", must be at least 8 characters long	Yes
--db-type	Type of database, which will be used (possible values: "MySQL Server", "Microsoft SQL Server")	
--db-driver	ODBC driver used for connecting to database (for example, "MySQL ODBC 5.3 ANSI Driver")	Yes
--db-hostname	Computer name or IP address of the database server	Yes
--db-port	Port of the database server (default 3306)	Yes
--db-name	Name of ERA Server database (default "era_db")	Yes
--db-admin-username	Database administrator username (used by installation for creating and modifying database)	Yes
--db-admin-password	Database administrator password	Yes
--db-user-username	Database ERA Server user username (usedby ERA Server for connecting to database); should be no longer than 16 characters	Yes
--db-user-password	Database ERA Server user password	Yes
--cert-hostname	Contains all the possible names and/or IP of the computer that ERA Server will be installed on. This will need to match with the server name specified in the Agent certificate that tries to connect to the server.	Yes
--server-cert-path	Path to server peer certificate (use this option if you specified --skip-cert as well)	
--server-cert-password	Password of server peer certificate	
--agent-cert-password	Password of Agent peer certificate	
--cert-auth-password	Certificate Authority password	
--cert-auth-path	Is the path to the Server's Certificate Authority file	
--cert-auth-common-name	Certification authority common name (use "")	
--cert-organizational-unit	-	
--cert-organization	-	
--cert-locality	-	
--cert-state	-	
--cert-country	-	
--cert-validity	Certificate validity in days or years (specify in argument --cert-validity-unit)	
--cert-validity-unit	Unit for certificate validity, possible values are 'Years' or 'Days' (default is Years)	
--ad-server	Active Directory server	No
--ad-user-name	Name of the user who has rights to search the AD network	No
--ad-user-password	Active Directory user password	No
--ad-cdn-include	Active Directory tree path, which will be synchronized for; use empty brackets "" to synchronize a whole tree	No

Installer log

The installer log may be useful for troubleshooting and can be found here:
`/var/log/eset/RemoteAdministrator/EraServerInstaller.log`

After installation verify whether the ERA Server service is running:
`service eraserver status`

3.8.1.1 Server prerequisites - Linux

The following prerequisites must be met in order to install ERA Server on Linux:

- A valid license.
- A Database Server already installed and configured, with a root account (a user account does not have to be created prior to the installation, the installer can create the account).
- An ODBC Driver for the connection to the database server (MySQL / MS SQL) installed on the computer.
  `apt-get install unixodbc libmyodbc` (Debian, Ubuntu distributions)
  `yum install mysql-connector-odbc` (CentOS, Red-Hat, Fedora distributions)

NOTE: You should use **unixODBC_23** package (not the default unixODBC) for ERA Server to connect to the MySQL database without any issues. This is especially true for SUSE Linux.

- Server installation file set as an executable.
  `chmod +x Server-Linux-i686.sh`
- The minimum supported version of openSSL is **openssl-1.0.1e-30**
- The **xvfb** package is required for proper report printing (Generate Report) on Linux Server systems without a graphical interface.
  `apt-get install xvfb` (Debian, Ubuntu distributions)
  `yum install xorg-x11-server-Xvfb` (CentOS, Red-Hat, Fedora distributions)
- The **cifs-utils** package is required for proper Agent deployment to a Windows OS.
  `apt-get install cifs-utils` (Debian, Ubuntu distributions)
  `yum install cifs-utils` (CentOS, Red-Hat, Fedora distributions)
- The **Qt4 WebKit libraries**: used for printing reports to PDF and PS format (must be version 4.8, not 5). All other **Qt4** dependencies will be installed automatically.
  `apt-get install libqtwebkit4` (Ubuntu distributions)

NOTE: In the case of CentOS, there may be no package in the official repositories. You can install it from a third-party repositorie (for example EPEL repositories) or compile it yourself on a target machine.

- The **kinit + klist** used for Kerberos authentication during the AD synchronization task and login with a domain user. Also a proper Kerberos configuration is required (*/etc/krb5.conf*).
  `apt-get install krb5-user` (Debian, Ubuntu distributions)
  `yum install krb5-workstation` (CentOS, Red-Hat, Fedora distributions)
- The **wbinfo + ntlm_auth** used for authentication with the domain accounts + NTLM authentication with SMTP server (sending emails)
  `apt-get install winbind` (Debian, Ubuntu distributions)
  `yum install samba-winbind-clients` (CentOS, Red-Hat, Fedora distributions)
- The **ldapsearch** used in AD synchronization task.
  `apt-get install ldap-utils` (Debian, Ubuntu distributions)
  `yum install openldap-clients` (CentOS, Red-Hat, Fedora distributions)
- The **snmptrap** used to send SNMP traps. Optional if this functionality won't be used. SNMP also requires configuration.
  `apt-get install snmp` (Ubuntu distributions)
  `yum install net-snmp-utils` (CentOS, Red-Hat, Fedora distributions)

- The **SELinux devel package** used during product installation to build SELinux policy modules. This is only required on systems with SELinux enabled (CentOS, Fedora, RHEL).
  `apt-get install selinux-policy-dev` (Debian, Ubuntu distributions)
  `yum install policycoreutils-devel` (CentOS, Red-Hat, Fedora distributions)

NOTE: ERA Server stores large data blobs in the database, therefore it is necessary to configure MySQL to accept large packet size for ERA to run properly. For details on how to configure this see FAQ.

3.8.2 Agent installation - Linux

Connection to the ERA Server is resolved using the parameters **--hostname** and **--port** (port is not used when an SRV record is provided). Possible connection formats are:

- **Hostname** and **port**
- **IPv4 address** and **port**
- **IPv6 address** and **port**
- Service record (SRV record) - to configure the DNS resource record in Linux, the computer must be in a domain with a working DNS server. See DNS resource record.

The SRV record must start with the prefix "_NAME._tcp" where 'NAME' represents custom naming (for example, 'era').

Below is a sample installation script, the parameters of this script are described in the following section.

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/admin/Desktop/agent.pfx --cert-auth-path=/h
--cert-password=N3lluI4#2aCC --hostname=10.1.179.36 --port=2222
```

`--skip-license` will cause the installer not ask the user for license confirmation
`--cert-path` is the path to the Agent certificate file
`--cert-auth-path` is the path to the Server's CA file
`--cert-password` must match the Agent's certificate password
`--hostname` is a connection to the server (or proxy) in one of these formats (Hostname, IPv4, IPv6 or SRV record)
`--port` is a listening, open port on the Server or Proxy (the default value for both is 2222)

Optional parameters:
`--product-guid` product GUID (if not defined, it will be generated)
`--cert-content` Base64 encoded content of PKCS12 encoded public key certificate plus private key used to set up secure communication channels with Server and Agents. Use only one of the `--cert-path` or `--cert-content` options.
`--cert-auth-content` Base64 encoded content of DER encoded certificate authority private key certificate used to verify remote peers (Proxy or Server). Use only one of the
`--cert-auth-path` or `--cert-auth-content` options.
`--webconsole-hostname` hostname used by webconsole to connect to the server (if left empty, value will be copied from 'hostname')
`--webconsole-port` port used by Web Console to connect to the server (default is '2223')
`--webconsole-user` username used by webconsole to connect to the server (default is 'Administrator')
`--webconsole-password` password used by webconsole to connect to the server

Connection and certificates

- **Connection to the ERA Server** must be provided: `--hostname`, `--port` (port is not needed if service record was provided, default is '2222')
- Provide these connection information for **Server-assisted installation**: --webconsole-port, --webconsole-user, --webconsole-password
- Provide certificate information for **Offline installation**: `--cert-path`, `--cert-password`

Password type parameters

Password type parameters can be provided as environment variable, file, read from stdin or provided as plain text, i.e.:
`--password=env:SECRET_PASSWORD` where SECRET_PASSWORD is environment variable with password
`--password=file:/opt/secret` where first line of regular file /opt/secret contains password
`--password=stdin` instructs installer to read password from standard input
`--password="pass:PASSWORD"` is equal to `--password="PASSWORD"` and is mandatory in case actual password is `"stdin"` or string starting with `"env:"`, `"file:"` or `"pass:"`

Installer log

The installer log may be useful for troubleshooting and can be found here:
`/var/log/eset/RemoteAdministrator/EraAgentInstaller.log`

To see if the installation was successful, verify that the service is running by executing the following command:
`sudo service eraagent status`

3.8.2.1 Agent prerequisites - Linux

The following prerequisites must be met in order to install ERA Agent component on Linux:

- ERA Server and ERA Web Console must be installed
- A Certificate for the Agent must be present
- A server Certification Authority public key file must be present
- The server computer must be reachable from the network
- The Agent installation file must be set as an executable (run chmod +x on the file to set this)
- Minimum supported version of openssl is **openssl-1.0.1e-30**

3.8.3 ERA Web Console installation - Linux

Before installing the ERA Web Console component, make sure all prerequisites are met:

1. Run the following commands to copy the *era.war* file into the selected folder:
   `sudo cp era.war /var/lib/tomcat/webapps/`
   Alternatively, you can extract the contents of era.war to `/var/lib/tomcat7/webapps/era/`
2. Run the following command to restart the Tomcat service and deploy the .war file, for example:
   `sudo service tomcat7 restart`
3. Open the following link in your browser on localhost (a login screen should be displayed):
   http://localhost:8080/era

NOTE: When you install the Web Console using the Installer, the default Web Console address is:

https://localhost/era/

3.8.3.1 ERA Web Console prerequisites - Linux

The following prerequisites must be met in order to install the ERA Web Console component on Linux:

- Java - always use the latest officially released version of Java (ERA Web Console requires at least Java version 7, but we strongly recommend to use the latest version)
  `apt-get install openjdk-7-jdk` (Debian, Ubuntu distributions)
  `yum install java-1.8.0-openjdk` (Red-Hat, Fedora distributions)
- Apache Tomcat (version 6 and newer)
  `sudo apt-get install tomcat7`
  `yum install tomcat7`
- Web Console file (*era.war*) saved to your local hard drive.

3.8.4 Proxy installation - Linux

1. Make sure all prerequisites are met.
2. Run an installation script to install the Proxy server. See an example of the installation script below.

Connection settings

A target must be specified with a:

- Hostname
- IPv4 address
- IPv6 address
- DNS resource record - The Linux computer must be in the domain - see the chapter DNS Resource record.

Port must be specified: use port 2222 both for Server and the Proxy.

Example of an installation
(New lines are split by "\" for copying the whole command to Terminal)

```
./Proxy-Linux-x86_64-1.0.407.0.sh --db-hostname=10.1.179.28 --db-dbname=era_6_db_proxy \
--db-admin-username=sa --db-admin-password=admin.1 --db-user-username=tester \
--db-user-password=Admin.1 --db-port=1433 --db-type="MS SQL Server" \
--db-driver=SQL --skip-license --hostname=10.1.179.30 --port=2222 \
--cert-path=/home/adminko/Desktop/proxy.pfx --cert-auth-path=/home/adminko/Desktop/CA-server.der \
--cert-password=root --server-root-password=jjf#jDjr
```

You can modify the following attributes:

`--db-hostname` is a hostname or IP address of the DB server
`--db-dbname` is a name of the database to be used
`--db-admin-username` is a DB administrator's name
`--db-admin-password` is a DB administrator's password
`--db-user-username` is a user, under which will the DB be accessed to
`--db-user-password` is the users password
`--db-port` is the port of the DB (1433 for MSSQL, 3306 for MySQL)
`--db-type` is the definition of used DB type (possible values "MySQL Server" and "MS SQL Server")
`--db-driver` must be set the same name as defined for MSSQL in the */etc/odbcinst.ini*
`--skip-license` will not ask the user for license confirmation
`--hostname` is a hostname or IP of the Server
`--port` is the Server port (by default 2222) or Proxy port (by default 1236)
`--proxy-port` Port which will be used by proxy (default value is "2222")
`--cert-path` is a local path to the Proxy certificate file
`--cert-auth-path` is a local path to Server's CA file
`--db-port` this setting is important and need to be specified if MySQL is used. If it is not specified, the default MySQL port 3306 is used.
`-product-guid` product GUID (if not defined, it will be generated)
`--cert-content` Base64 encoded content of PKCS12 encoded public key certificate plus private key used to set up secure communication channels with Server and Agents.
Use only one of the `--cert-path` or `--cert-content` options.
`--cert-password` must match the Agent's certificate password
`--cert-auth-content` Base64 encoded content of DER encoded certificate authority private key certificate used to verify remote peers (Proxy or Server). Use only one of the
`--cert-auth-path` or `--cert-auth-content` options.
`--keep-database` database will not be removed during uninstallation

To verify whether the installation was successful, use the following command to verify whether the service is running:

```
sudo service eraproxy status
```

3.8.4.1 Proxy prerequisites - Linux

The following prerequisites must be met in order to install Proxy component on Linux:

- **ERA Server** and the **ERA Web Console** installed (on a Server computer).
- An ODBC Driver for the connection to the Database Server (MySQL / MS SQL) installed on the computer.
- A Database Server already installed and configured.
- **Proxy Certificate** created and downloaded to your local drive.
- **Certificate Authority** prepared on your local drive.
- A valid license.
- Agent must be installed on a local computer to fully support all program features.
- Minimum supported version of openssl is **openssl-1.0.1e-30**

3.8.5 RD Sensor installation and prerequisites - Linux

To install the RD Sensor component on Linux, follow these steps:

1. Make sure the following prerequisites are met:
   - The Network can be searched (ports are open, the firewall is not blocking incoming communication, etc.).
   - The Server computer can be reached.
   - ERAgent must be installed on the local computer to fully support all program features.
   - The Terminal is open.
2. Use the following command to run the installation file as sudo:

```
sudo ./RDSensor-Linux-x86_64-1.0.223.0.sh
```

3. To see if the installation was successful, verify that the service is running by executing the following command:

```
sudo service rdsensor status
```

4. Rogue Detection Sensor will be installed on your computer.
5. The Rogue Detection Sensor log file can be found in: *var/log/eset/RemoteAdministrator/RogueDetectionSensor/trace.log*

3.8.6 Mobile Device Connector installation - Linux

You can install Mobile Device Connector on a different server than the one on which your ERA Server is running. For example if you want to make Mobile Device Connector accessible from the internet so that the user's mobile devices can be managed at all times.

Installation of the ERA Server component on Linux is performed using a command in the Terminal. Make sure all prerequisites are met. You can prepare an installation script and then execute it using *sudo*.

There are many optional installation parameters, but some of them are required.

Your ERA Peer Certificate is required for installation. There are two methods to get the ERA peer certificate:

- **Server assisted installation** - you'll need to provide ERA Web Console administrator credentials (installer will download required certificates automatically).
- **Offline installation** - you'll need to provide a peer certificate (the Agent certificate exported from ESET Remote Administrator). Alternatively, you can use your custom certificate.

Installation command parameters that must be provided:

HTTPS certificate:

```
--https-cert-path=
--https-cert-password=
```

Peer Certificate:
For a **Server assisted installation** at least include:

```
--webconsole-password=
```

For an **Offline installation** include:

`--cert-path=`

`--cert-password=` (password is not needed for the default Agent Certificate created during initial ERA Server installation)

Connection to ERA Server (name or IP address):

`--hostname=`

For a MySQL database include:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

For a MSSQL database include:

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

If a MySQL/MSSQL database already existing, include either:

`--db-use-existing-db=`

or

`--db-drop-existing-db=`

Example

(New lines are split by "\" for copying the whole command to Terminal)

```
sudo ./MDMCore-Linux-x86_64-0.0.0.0.sh \
--https-cert-path="./httpscert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--db-use-existing-db \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

For a complete list of available parameters (print help message), use:

`--help`

Installer log

The installer log may be useful for troubleshooting and can be found here:

`/var/log/eset//mdminstaller.log`

After installation is complete, check to see if the Mobile Device Connector is running correctly by opening https://*your-mdm-hostname*:*enrollment-port* (for example *https://eramdm:9980*) in your web browser. If the installation was successful, you'll see following message:

MDM Server up and running!

You can also use this URL to check the availability of the Mobile Device Connector server from the internet (if configured in such a way) by visiting it from a mobile device. If you are unable to reach the page, check your firewall and the configuration of your network infrastructure.

3.8.6.1 Mobile Device Connector prerequisites - Linux

The following prerequisites must be met in order to install Mobile Device Connector on Linux:

- A Database Server already installed and configured with a root account (a user account doesn't have to be created prior to installation, the installer can create the account).
- An ODBC Driver for the connection to the database server (MySQL / MS SQL) installed on the computer.
  `apt-get install unixodbc libmyodbc` (Debian, Ubuntu distributions)
  `yum install mysql-connector-odbc` (CentOS, Red-Hat, Fedora distributions)

NOTE: You should use **unixODBC_23** package (not the default unixODBC) in order for the ERA Server to connect to the MySQL database without any issues. This is especially true for SUSE Linux.

  - Server installation file set as an executable.
    `chmod +x MDMCore-Linux-i686.sh`
  - After installation, verify that MDMCore service is running.
    `service mdmcore status`
  - The minimum supported version of openSSL is **openssl-1.0.1e-30**

NOTE: ERA Server stores large data blobs in the database, therefore it is necessary to configure MySQL to accept large packet size for ERA to run properly. For details on how to configure this, see our FAQ.

IMPORTANT: You'll need an **SSL certificate** in `.pfx` format for secure communication over HTTPS. We recommend that you use a certificate provided by a Certificate Authority (CA). Self-signed certificates are not recommended because not all mobile devices let users to accept self-signed certificates. This isn't an issue with CA signed certificates, because they are trusted and do not require acceptance by the user.

IMPORTANT: For Offline installation, you'll also need a peer certificate (the **Agent certificate** exported from ESET Remote Administrator). Alternatively, you can use your custom certificate with ERA.

3.8.7 Apache HTTP Proxy installation - Linux

To install the Apache HTTP Proxy component on Linux, follow these steps:

1. Install Apache HTTP Server (at least version 2.4.10)
2. Load following modules: access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile, authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
3. Add caching configuration:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. If the directory */var/cache/apache2/mod_cache_disk* does not exist, create it and assign Apache privileges (r,w,x)
5. Add proxy configuration:

```
ProxyRequests On
ProxyVia On

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Enable the added configuration (if configuration is in main conf, you can skip this step)
7. If required, change listening to your desired port (port 3128 is set by default)
8. Optional basic authentication:
   - Add authentication configuration to the proxy directive:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

   - Create a password file using `htpasswd.exe -c`
   - Manually create a file named group.file with `usergroup:username`
9. Restart the server

Ubuntu server 14.10:

1. `sudo apt-get install apache2`
2. `sudo a2enmod access_compat auth_basic authn_core authn_file authz_core authz_groupfile authz_host proxy proxy_http proxy_connect cache cache_disk`
3. `sudo vim /etc/apache2/conf-available/caching.conf`
   - copy/paste caching configuration:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. This step should not be required, but if the caching directory is missing, run following commands:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. `sudo vim /etc/apache2/conf-available/proxy.conf`
   - copy/paste proxy configuration:

```
ProxyRequests On
ProxyVia On

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. `sudo a2enconf caching.conf proxy.conf`
7. `sudo vim /etc/apache2/ports.conf`
   - replace `Listen 80` with `Listen 3128`
8. Optional basic authentication:
   - `sudo vim /etc/apache2/conf-available/proxy.conf`
     - copy/paste authentication configuration before `</Proxy>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

- install apache2-utils and create password file:

```
sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user
```

- create file with groups:

```
sudo vim /etc/apache2/group.file
copy/paste usergroup:user
```

9.sudo service apache2 restart

General settings:

Allow forwarding for ESET communication only:

1. Replace the following in proxy configuration:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

with:

```
<Proxy *>
Deny from all
</Proxy>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.
[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.
[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.
mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net|edf-pcs.cloudapp.net|edf-pcs2.clouda
edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?(87.106.247.14|209.157.66.250|209.157.66.253|
212.227.134.125|212.227.134.126|212.227.134.128|212.227.134.130|212.227.134.131|212.227.134.132|
212.227.134.133|212.227.134.158)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
```

Proxy chaining (all traffic):

Add the following to the proxy configuration (password is working only on child proxy):

```
ProxyRemote * http://10.1.172.26:3128
```

3.8.7.1 Squid

Ubuntu server 14.10:

1.sudo apt-get install squid3

2.sudo vim /etc/squid3/squid.conf

replace `#cache_dir ufs /var/spool/squid3 100 16 256` with `cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000`

3.sudo service squid3 stop

```
sudo squid3 -z
```

4.sudo vim /etc/squid3/squid.conf

Add `http_access allow all` before `http_access deny all` to allow all to access proxy

5.sudo service squid3 restart

Squid3:

1. Install Squid3
2. Add `cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000` to your configuration under `cache_dir` (5000 is cache size in MB)
3. Create a caching folder with squid: `squid3 -z` (stop squid3 service if it is running)
4. Allow access for desired clients
5. Restart squid3

3.8.8 How to uninstall or reinstall a component - Linux

If you want to reinstall or upgrade to a more recent version, run the installation script again.

To uninstall a component (in this case ERA Server), run the installer with the **--uninstall** parameter, as shown below:
`sudo ./Server-Linux-i686.sh --uninstall --keep-database`

If you want to uninstall other component, use appropriate package name in the command. For example ERA Agent:
`sudo ./Agent-Linux-x86_64.sh --uninstall`

Warning: Configuration and database files will be removed during uninstallation. To preserve database files, create a SQL dump of the database or use the `--keep-database` parameter.

After uninstall check

- service `eraserverService.sh` is deleted.
- folder `/etc/opt/eset/RemoteAdministrator/Server/` is deleted.

We recommend that you create a database dump backup before performing uninstallation in case you need to restore your data.

3.9 DNS Service Record

To set up a DNS Resource Record:

1. On your DNS Server (DNS server on your Domain controller), navigate to **Control Panel** > **Administrative Tools**.
2. Select the DNS value.
3. In the DNS Manager, select *_tcp* from the tree and create a new **Service location (SRV**) record.
4. Enter the service name in the **Service** field according to DNS standard rules, type an underline symbol (**_**) in front of the service name (use your own service name, for example **_era**).
5. Enter the tcp protocol in the **Protocol** field in the following format: *_tcp*.
6. Enter the port 2222 in the **Port number** field.
7. Enter the ERA Server fully qualified domain name (FQDN) in the **Host offering this service** field.
8. Save the record by clicking [**OK**], and then [**Done**] - the record will be displayed in the list.

To verify the DNS record:

1. Log into any computer in your domain and open a command prompt (*cmd.exe*).
2. Type *nslookup* into the command prompt and press **Enter**.
3. Type *set querytype=srv* and press **Enter**.
4. Type *_era._tcp.domain.name* and press **Enter**. The service location is displayed correctly.

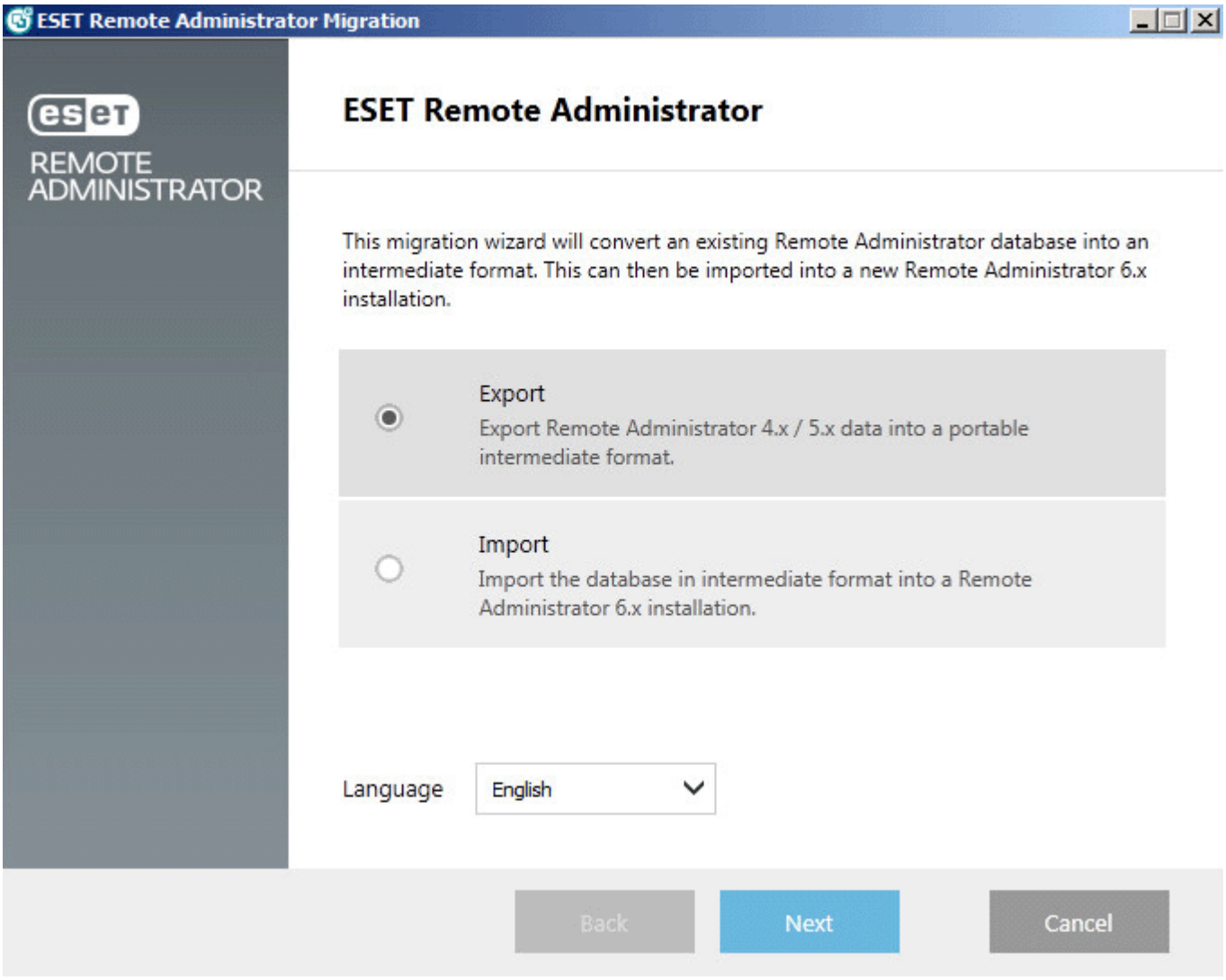
NOTE: This procedure is the same for Windows and Linux.

NOTE: Don't forget to change the "Host offering this service:" value to the FQDN of your new server when you install ESET Remote Administrator Server on a different machine.

3.10 Migration Tool

The migration wizard is a standalone application that provides straightforward migration of ERA 4.x / 5.x data into an intermediate database and allows you to import it into ERA 6.x.

Download the ESET Remote Administrator Migration Tool. You will need existing ESET-issued Username and Password to download the tool.

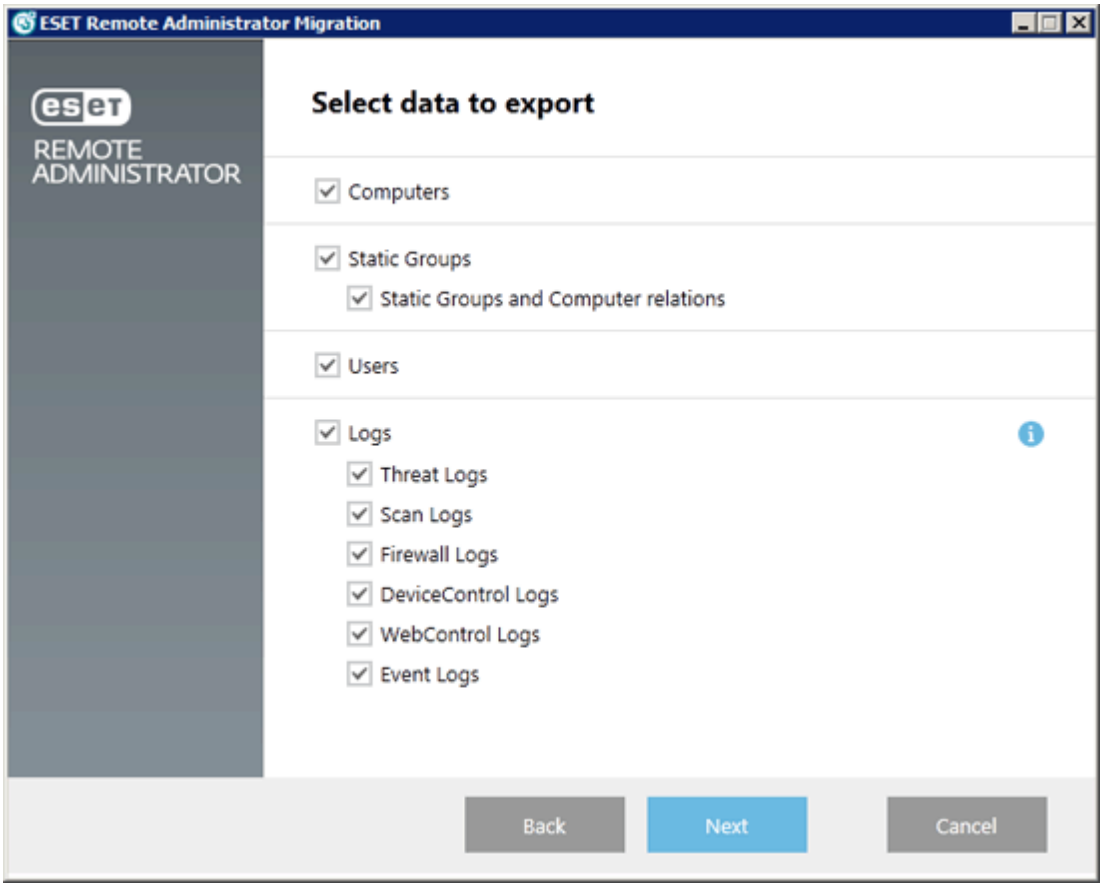

ESET Remote Administrator Migration
REMOTE ADMINISTRATOR
ESET Remote Administrator
This migration wizard will convert an existing Remote Administrator database into an intermediate format. This can then be imported into a new Remote Administrator 6.x installation.
Export
Export Remote Administrator 4.x / 5.x data into a portable intermediate format.
Import
Import the database in intermediate format into a Remote Administrator 6.x installation.
Language
English
Back
Next
Cancel

NOTE: To resolve a problem with missing `MSVCP100.dll` or `MSVCR100.dll` files, install the latest Microsoft Visual C++ 2010 Redistributable Package. You can use the following link Microsoft Visual C++ 2010 Redistributable Package (x86).

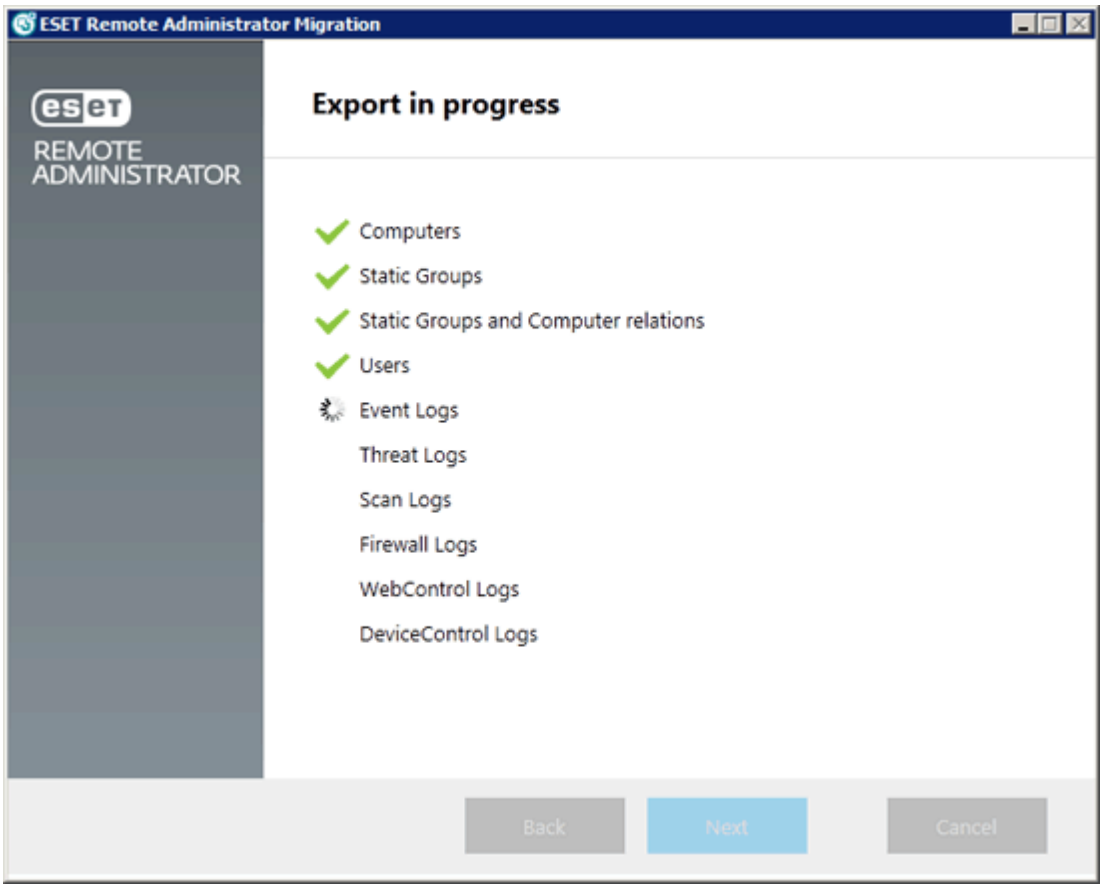
3.10.1 Migration scenario 1

This scenario covers migration to ERA 6.x running on a different computer than ERA 4.x / 5.x.

1. The first step in the migration process is to have ERA 6.x installed and running on another computer.
2. Start the ESET Remote Administrator Migration tool on the ERA 4.x / 5.x machine and select **Export** to save the data from the old ERA to an intermediate database file.
3. Migration wizard is able to transfer specific data only. Select the data you want to transfer and click **Next**.



Because of the new design and function of Dynamic Groups in ERA 6.x, it is not possible to transfer parametric groups, tasks and policies from earlier versions. After you have selected a folder in which to save the temporary database, the wizard will display the status of archival of the ERA 4.x / 5.x database.



All data is exported to an **intermediate database**.

4. When data is finished exporting, there are two options you can choose from:
   - One option is to **Finish** the export, **Copy** the temporary database file to a server that is running ESET Remote Administrator 6.x, and import the data using the ERA Migration tool on that server.
   - A second option is to click **Import now** and import the data directly to ESET Remote Administrator 6.x over the network. Specify the connection and logon details of the new ERA Server.

NOTE: Static groups synchronized from Active Directory are ignored and will not be exported.

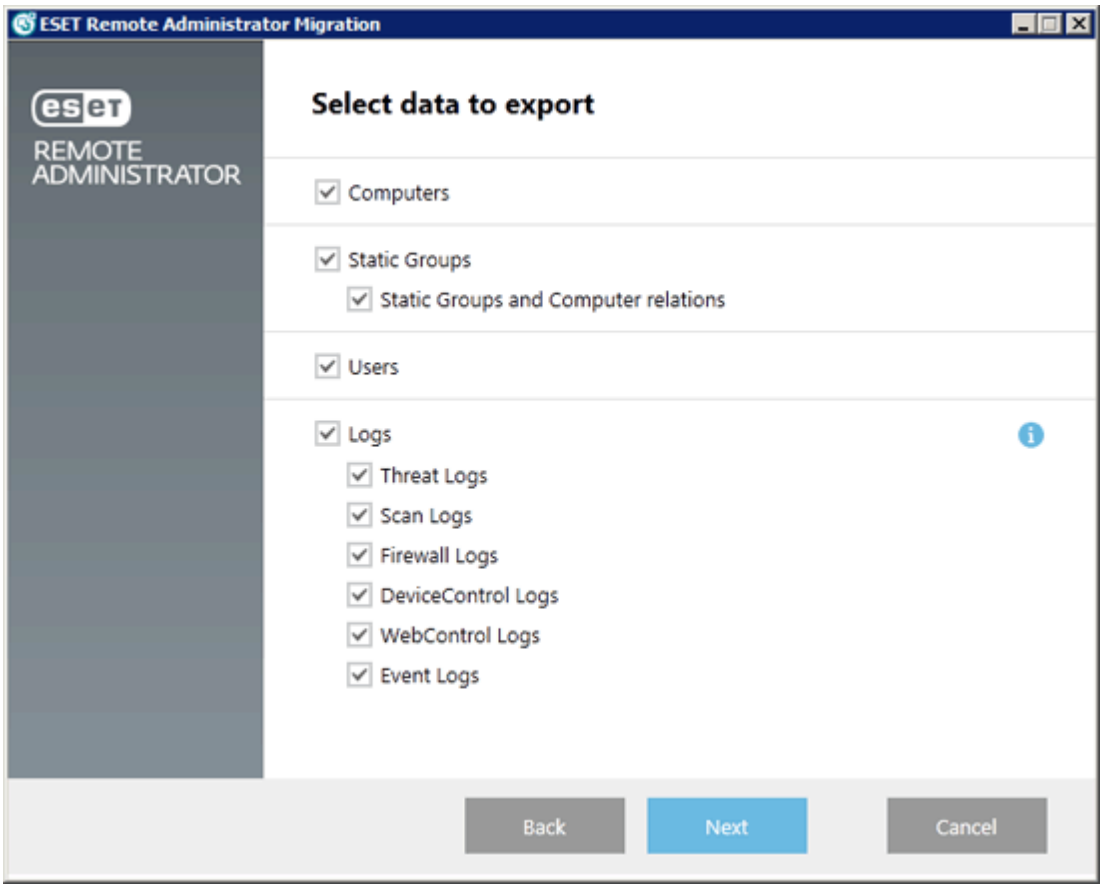
- If server settings won't allow for importation of specific data, the ESET Remote Administrator Migration tool will let you choose whether you want to change settings in ERA 6.x for specific components.
- Each of the components is then imported. An **import (migration) log** is available for each component. After the import is complete, the Migration tool will display the results of the import process.
- If you chose to migrate users, their passwords were reset and replaced with randomly generated passwords. These passwords can be exported in the `.csv` format.
- The migration tool wizard also generates a script that can be used to preconfigure ERA Agents on client machines. This script is a small executable `.bat` file distributable to client computers.
- We recommend that you review migrated settings and data to make sure that importation was successful. After checking, use this script to deploy the ERA Agent on a small group of computers to check if they are connecting to the server correctly.
- After the successful connection of the test group, you can deploy the Agent to the remaining computers (either manually or using an AD synchronization task).

NOTE: If any of the migration steps fail you should roll back changes for ERA 6.x, setup the computers to connect to ERA 4.x / 5.x, recover the backup data from ERA 4.x / 5.x and contact ESET customer care.

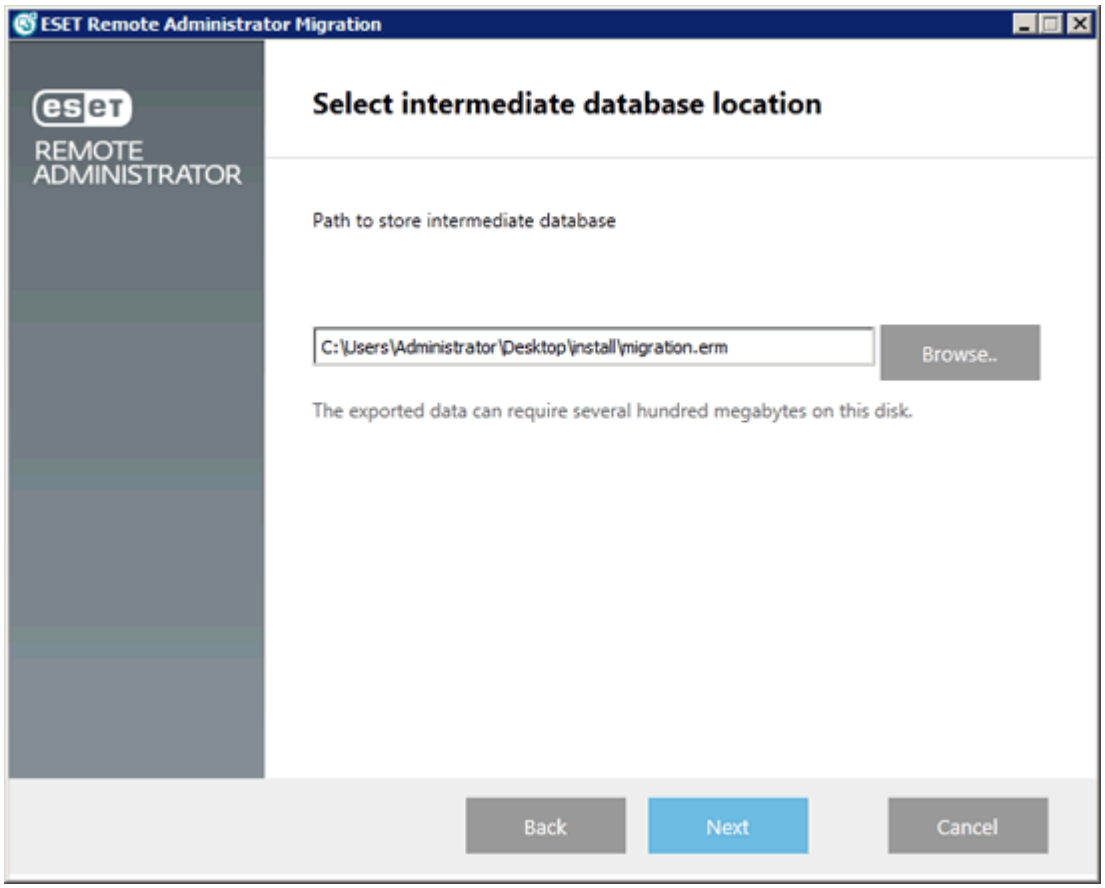
3.10.2 Migration scenario 2

This scenario covers migration to ESET Remote Administrator 6.x running on the same computer as ERA 4.x / 5.x. All ERA data should be backed up (using the ESET Maintenance tool) and ERA services in the operating system should be stopped before the migration of any data.

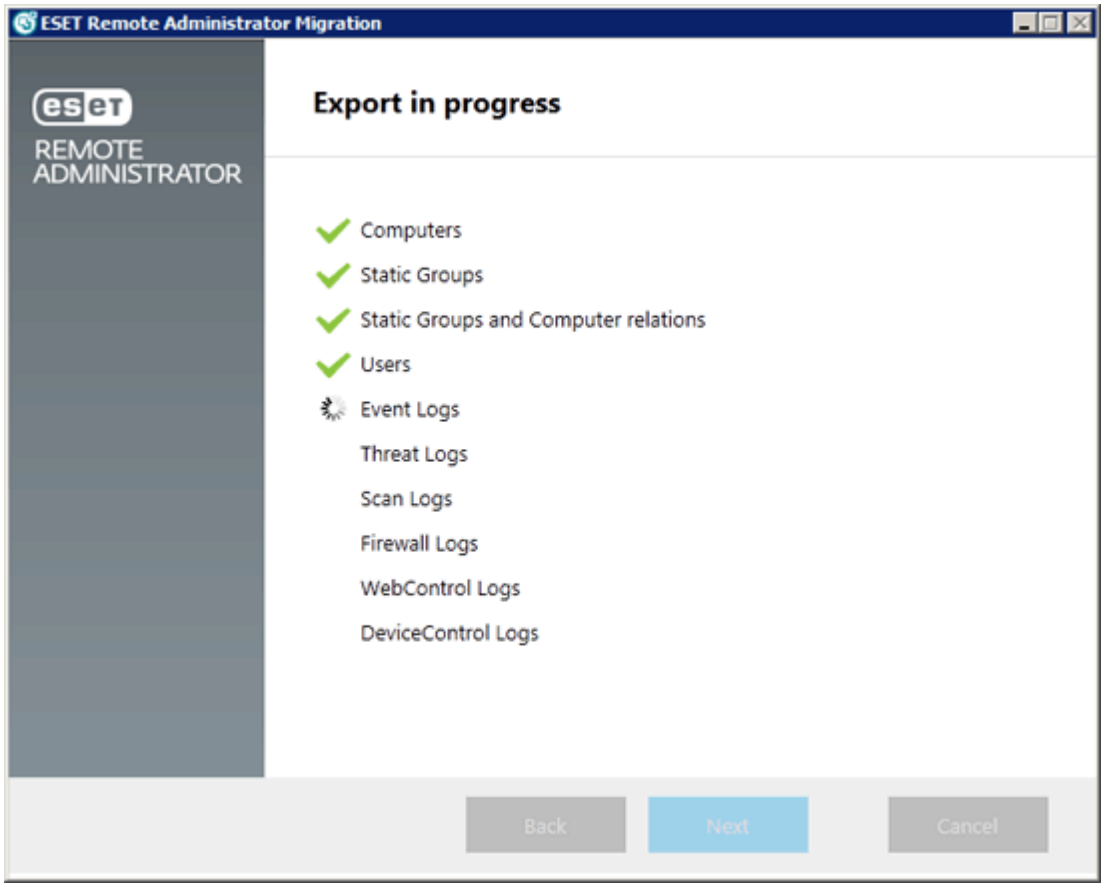
1. After running the ESET Remote Administrator Migration tool on the ERA 4.x / 5.x machine, the administrator selects the **Export** option to save the data from ERA 4.x / 5.x to an intermediate database file. Migration wizard is able to transfer specific data only:



NOTE: It is not possible to transfer parametric groups, tasks and policies from ERA 4.x / 5.x, because of the new design and functions of Dynamic Groups in ERA 6.x.



2. After selecting a save folder for the temporary database, the wizard will display the status of archival of the ERA 4.x / 5.x database.



3. All data is exported to an **intermediate database**.

- After the successful data **export** and before ERA 6.x **deployment**, ERA 4.x / 5.x must be **uninstalled**.
- When new ERA 6.x is installed, exported database can be imported using the Migration tool. Administrator is prompted to select the saved file.
- If server settings won't allow for importation of specific data, the ESET Remote Administrator Migration tool will let you choose whether you want to change settings in ERA 6.x for specific components.
- Each of the components is then imported. An **import (migration) log** is available for each component. After the import is complete, the Migration tool will display the results of the import process.
- If you chose to migrate users, their passwords were reset and replaced with randomly generated passwords. These passwords can be exported in the `.csv` format.
- The migration tool wizard also generates a script that can be used to preconfigure ERA Agents on client machines. This script is a small executable `.bat` file distributable to client computers.
- We recommend that you review migrated settings and data to make sure that importation was successful. After checking, use this script to deploy the ERA Agent on a small group of computers to check if they are connecting to the server correctly.
- After the successful connection of the test group, you can deploy the Agent to the remaining computers (either manually or using an AD synchronization task).

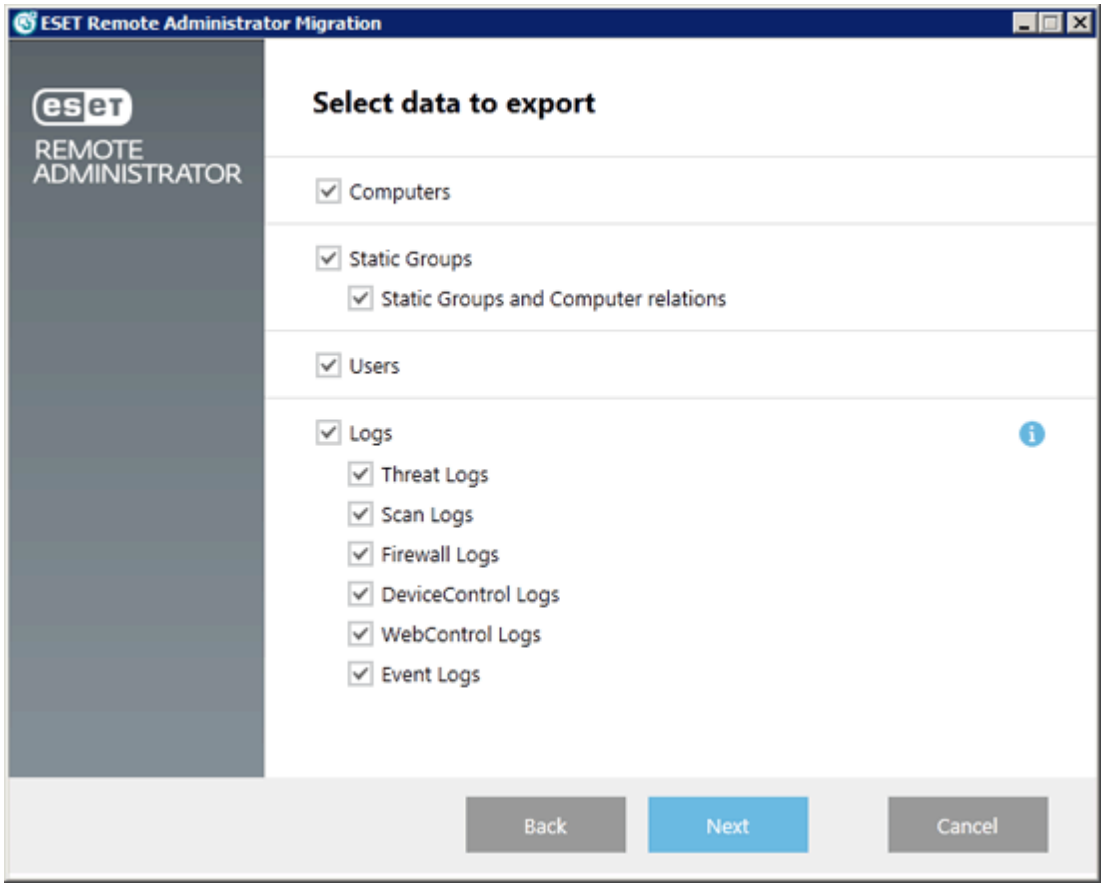
NOTE: If any of the migration steps fail you should roll back changes for ERA 6.x, setup the computers to connect to ERA 4.x / 5.x, recover the backup data from ERA 4.x / 5.x and contact ESET customer care.

3.10.3 Migration scenario 3

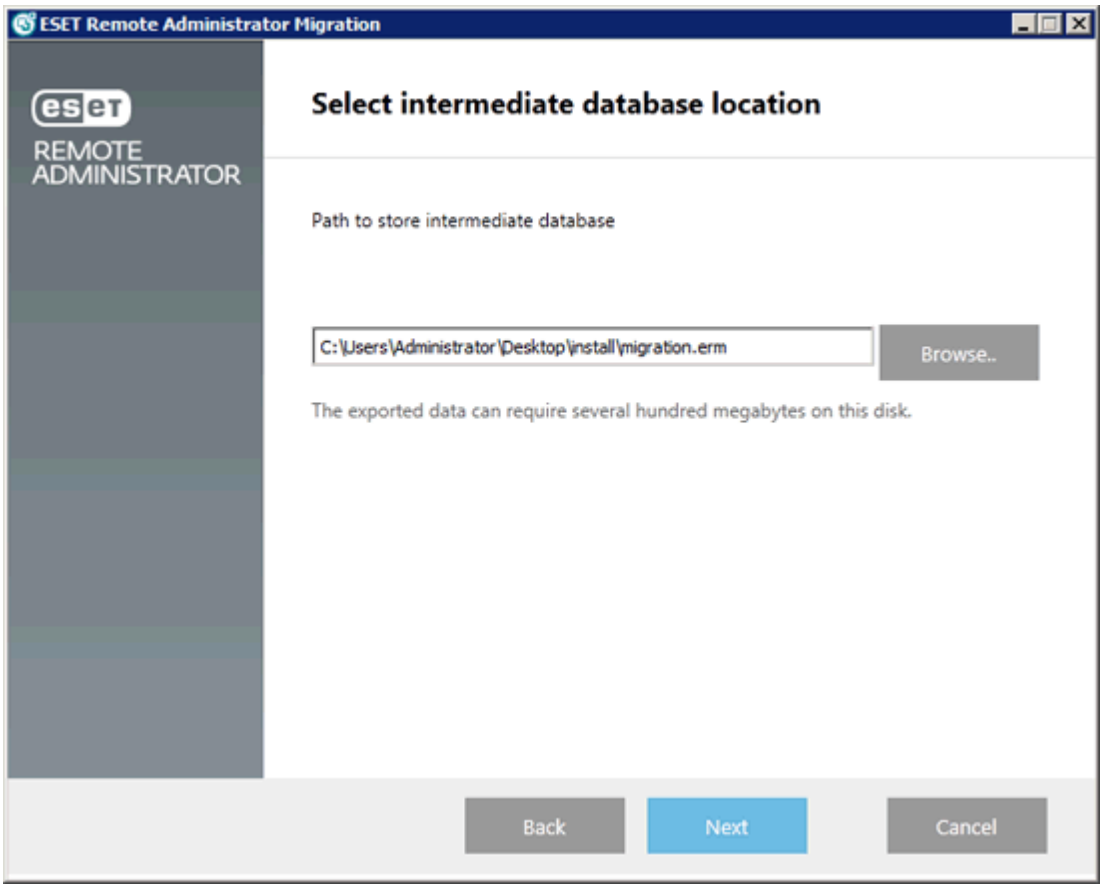
This scenario covers a migration to ERA 6.x where endpoints connect to old ERA 4.x / 5.x until the ERA Agent is deployed by ERA 6.x.

NOTE: This scenario is for highly skilled users only. We do not recommend this type of migration unless there is no other option.

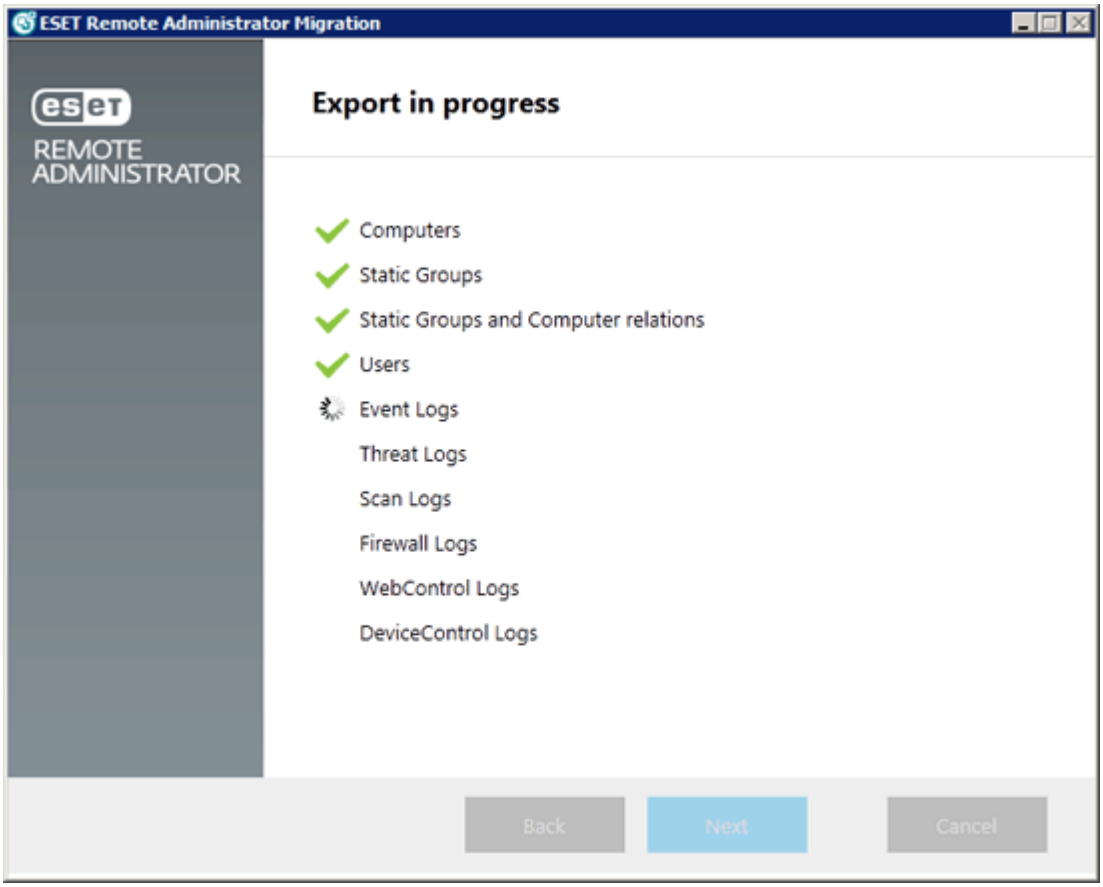
1. After running the ESET Remote Administrator Migration tool on the ERA 4.x / 5.x machine, the administrator selects the **Export** option to save the data from ERA 4.x / 5.x to an intermediate database file. Migration wizard is able to transfer specific data only:



NOTE: It is not possible to transfer parametric groups, tasks and policies from ERA 4.x / 5.x, because of the new design and functions of Dynamic Groups in ERA 6.x.



2. After selecting a save folder for the temporary database, the wizard will display the status of archival of the ERA 4.x / 5.x database.



3. All data is exported to an **intermediate database**.

4. If ERA 6 will be installed on the same computer as 4.x / 5.x, you must change your old ERA ports and rename the server service (`sc config ERA_SERVER DisplayName= "ESET Remote Administrator g1"`).
5. ESET Remote Administrator 4.x / 5.x should be started again following the export of your data.
6. Install ESET Remote Administrator 6 and import the intermediate database using the Migration tool.
    - If server settings won't allow for importation of specific data, the ESET Remote Administrator Migration tool will let you choose whether you want to change settings in ERA 6.x for specific components.
    - Each of the components is then imported. An **import (migration) log** is available for each component. After the import is complete, the Migration tool will display the results of the import process.
    - If you chose to migrate users, their passwords were reset and replaced with randomly generated passwords. These passwords can be exported in the `.csv` format.
    - The migration tool wizard also generates a script that can be used to preconfigure ERA Agents on client machines. This script is a small executable `.bat` file distributable to client computers.
    - We recommend that you review migrated settings and data to make sure that importation was successful. After checking, use this script to deploy the ERA Agent on a small group of computers to check if they are connecting to the server correctly.
    - After the successful connection of the test group, you can deploy the Agent to the remaining computers (either manually or using an AD synchronization task).

NOTE: If any of the migration steps fail you should roll back changes for ERA 6.x, setup the computers to connect to ERA 4.x / 5.x, recover the backup data from ERA 4.x / 5.x and contact ESET customer care.

The consequence of this type of migration is that there won't be any logs exported between the process of backing up the ERA 4.x / 5.x database and deploying the Agent on a client computer. However that data will still be present on your old copy of ERA 4.x / 5.x.

4. First Steps

After you have successfully installed ESET Remote Administrator you can move on to setting things up. The following chapters will show you the recommended initial steps that should be taken after the installation of ESET Remote Administrator.

First, open ERA Web Console in your web browser and log in.

Getting to know ERA Web Console

Before you begin initial setup, we recommend that you get to know the ERA Web Console, as it is the interface which you will be using to manage ESET security solutions.

Adding client computers, servers and mobile devices on your network to ERA structure
During installation, you can choose to search your network for computers (clients), all clients found will be listed in the **Computers** section when you start ESET Remote Administrator. If clients are not shown in the **Computers** section, run the Static Group Synchronization task to search for computers and show them in groups.

Deploying an Agent
Once the computers are found, deploy the Agent on the client computers. The Agent provides communication between ESET Remote Administrator and clients.

Installing ESET product (including activation)
To keep your clients and network secure, install ESET products. This is done using the Software Install task.

Creating/editing groups
We recommend that you sort clients into Groups, either static or dynamic, based on various criteria. This makes managing clients easier and helps you keep an overview of your network.

Creating a new policy
Policies are very useful if you want to push a specific configuration of an ESET product that is running on your client computers. This allows you to avoid configuring each client's ESET product manually, by enforcing the configuration using a policy. Once you have created a new policy with your custom configuration, you can assign it to a group (either static or dynamic). Then the policy is applied to all the computers in that group.

Assigning policy to a group
As explained above, in order for a policy to be applied it needs to be assigned to a group. Computers that belong to the group will have this policy applied to them. The policy is applied every time an Agent connects to ERA Server.

Setting up Notifications and creating Reports
To keep a better overview of what is going on with client computers in your environment, we recommend that you use notifications and reports, for example if you want to be notified that a certain event occurred or want to see or download a report.

4.1 Opening the ERA Web Console

There are multiple ways to open the ERA Web Console:

- On your local server (the machine hosting your Web Console) type this URL into the web browser:
  https://localhost/era/

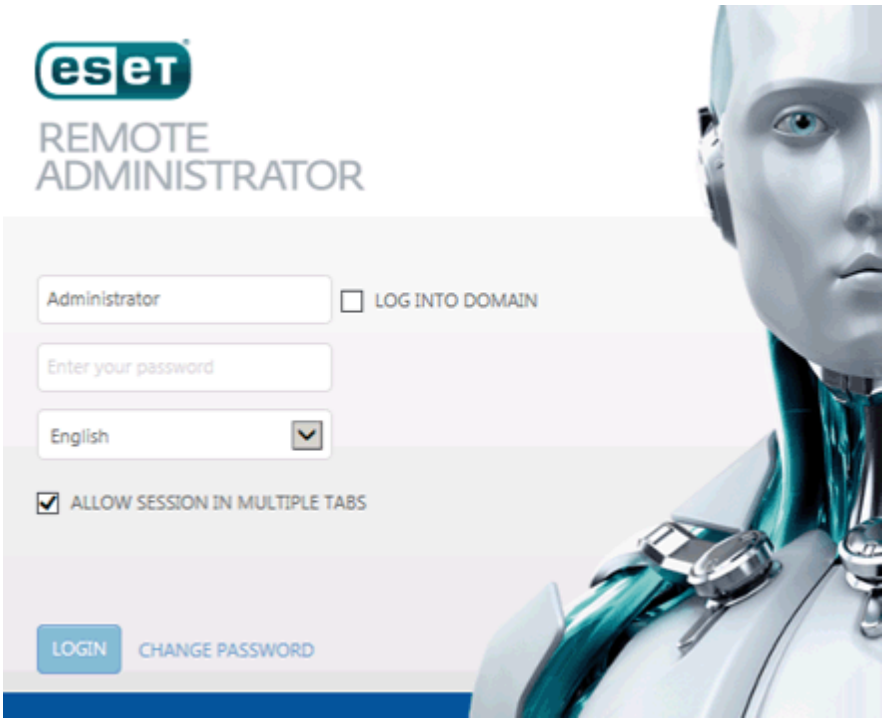
- From any place with internet access to your web server, type the URL in following format:
  https://yourservername/era/
  Replace "yourservername" with the actual name or IP address of your web server.

- To log into the ERA Virtual appliance, use following URL:
  https://[IP address]:8443/
  Replace "[IP address]" with the IP address of your ERA VM. If you do not remember the IP address, see step 9 of Virtual appliance deployment instructions.

- On your local server (the machine hosting your Web Console), click **Start** > **All Programs** > **ESET** > **ESET Remote Administrator** > **ESET Remote Administrator Webconsole** - a login screen will open in your default web browser. This does not apply to the ERA Virtual appliance.

NOTE: Since the Web Console uses secure protocol (HTTPS), you might get a message in your web browser regarding a security certificate or untrusted connection (exact wording of the message depends on the browser you are using). This is because your browser wants you to verify the identity of the site you are trying to access. Click **Continue to this website** (Internet Explorer) or **I Understand the Risks**, click **Add Exception...** and then click **Confirm Security Exception** (Firefox) to allow access to the ERA Web Console. This only applies when you're trying to access the ESET Remote Administrator Web Console URL.

When web server (that runs ERA Web Console) is up, the following screen is displayed.

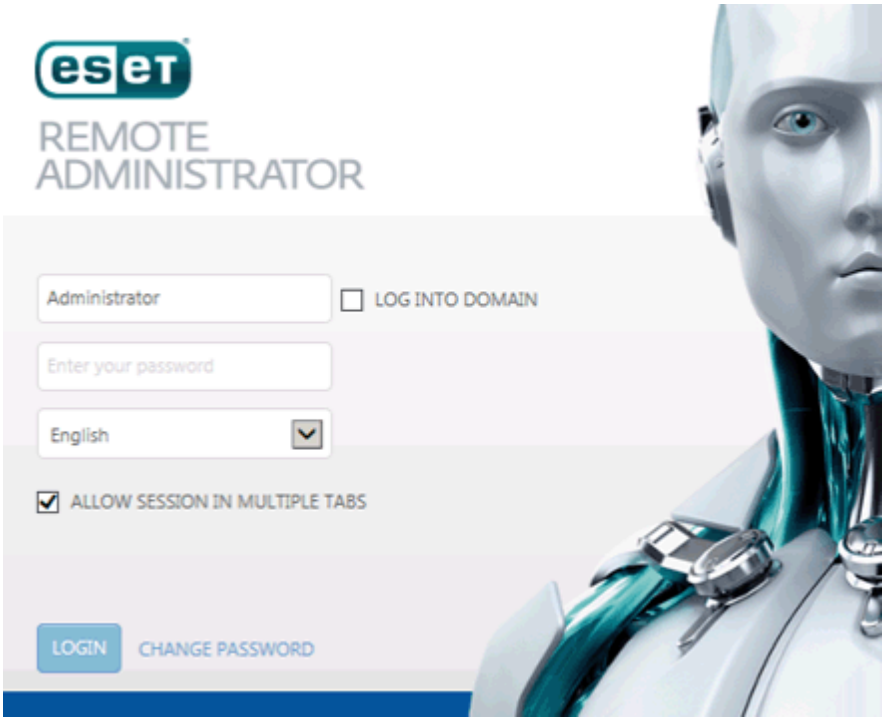


If this is your first login, please provide the credentials you entered during the Installation process. For more details about this screen, see Web Console login screen.

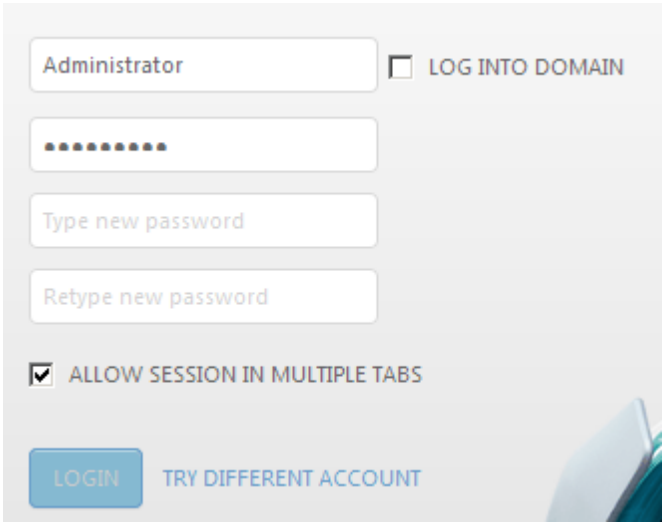
NOTE: In the rare case that you do not see the login screen or when the login screen appears to be constantly loading, restart the *ESET Remote Administrator Server* service. Once the *ESET Remote Administrator Server* service is up and running again, restart the *Apache Tomcat* service. After this, the Web Console login screen will load successfully.

4.2 The ERA Web Console login screen

A user needs login credentials (username and password) to log into the Web Console. It is also possible to log in as a domain user by selecting the check box next to **Log into domain** (a domain user is not related to any mapped domain group). You can select your language from a list in the top right corner of the login screen. Select **Allow session in multiple tabs** to allow users to open ERA Web Console in multiple tabs in your web browser.



Change Password / **Try different Account** - allows you to change password or switch back to login screen. A user without a permission set is allowed to log into the Web Console, but he will not see any relevant information.



To give a user read/write/modify permissions in Web Console modules, a proper Permission Set must be created and assigned to the user.

Session management and security measures:

- **Login IP address lockout**

After 10 unsuccessful login attempts from the same IP address, further login attempts from this IP address are temporarily blocked for approximately 10 minutes. The IP address ban on login attempts does not affect existing sessions.

- **Wrong session ID address lockout**

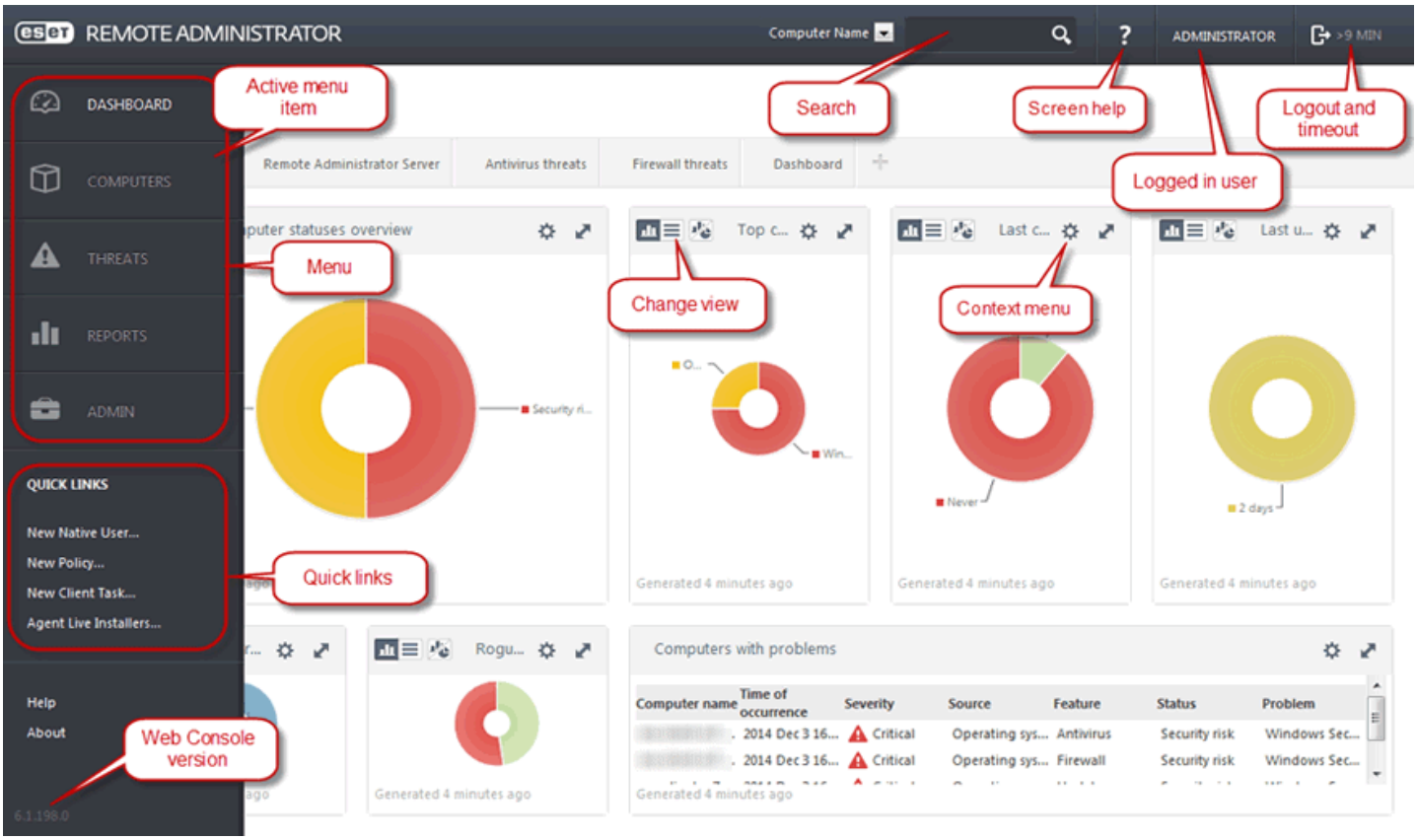
After using an invalid session ID 15 times from the same IP address, all further connections from this IP address are blocked for approximately 15 minutes. Expired session IDs are not counted in. If there is an expired session ID in the browser, it is not considered an attack. The 15-minute IP address ban is for all actions (including valid requests).

4.3 Getting to know ERA Web Console

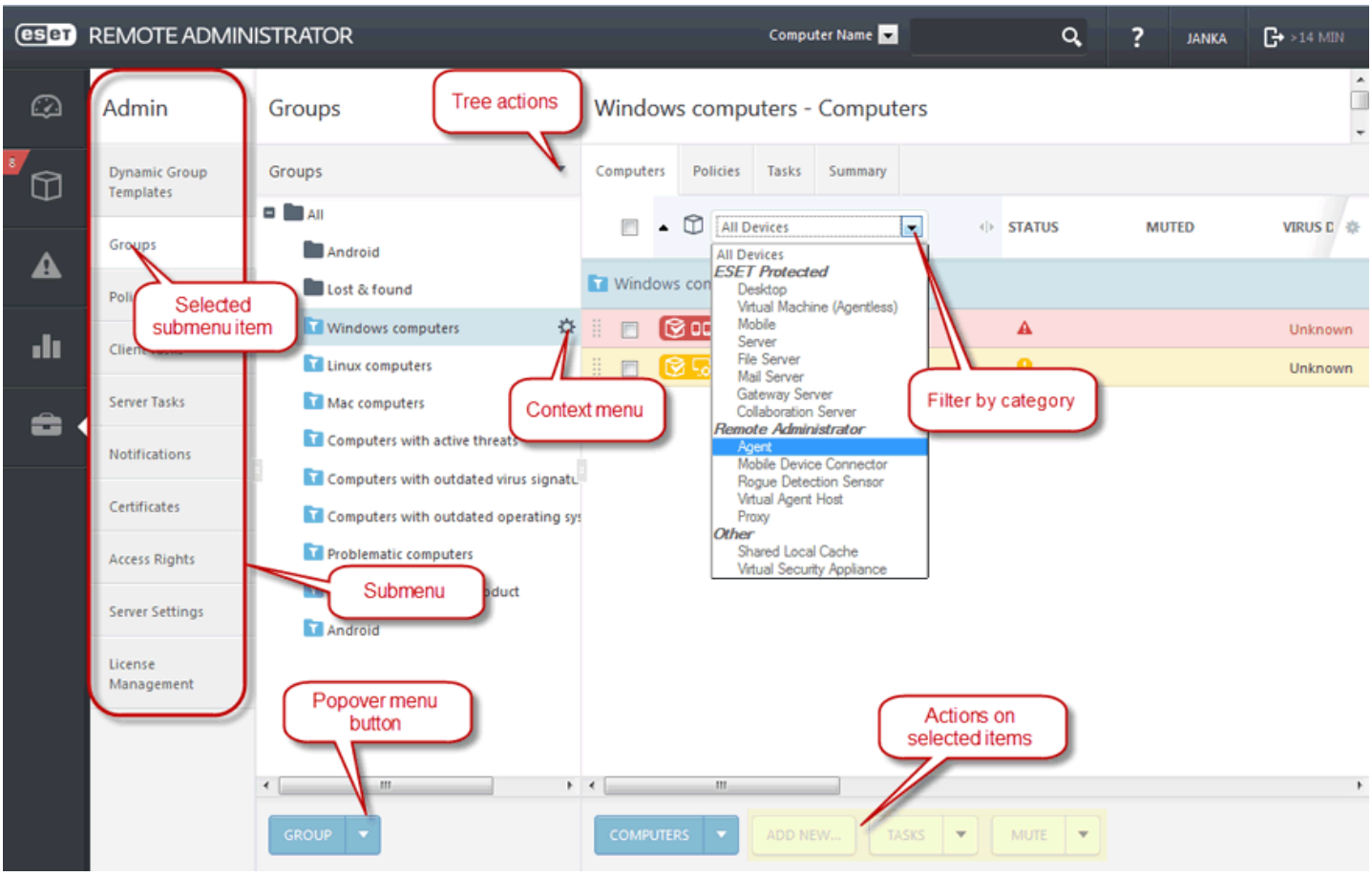
ESET Remote Administrator Web Console is the main interface which connects to the ERA Server. You can think of it as a control panel, a central place from which you can manage all of your ESET security solutions. It is a web-based interface which can be accessed using a browser (see Supported Web browsers) from any place and any device with internet access.

The basic principles in GUI orientation are:

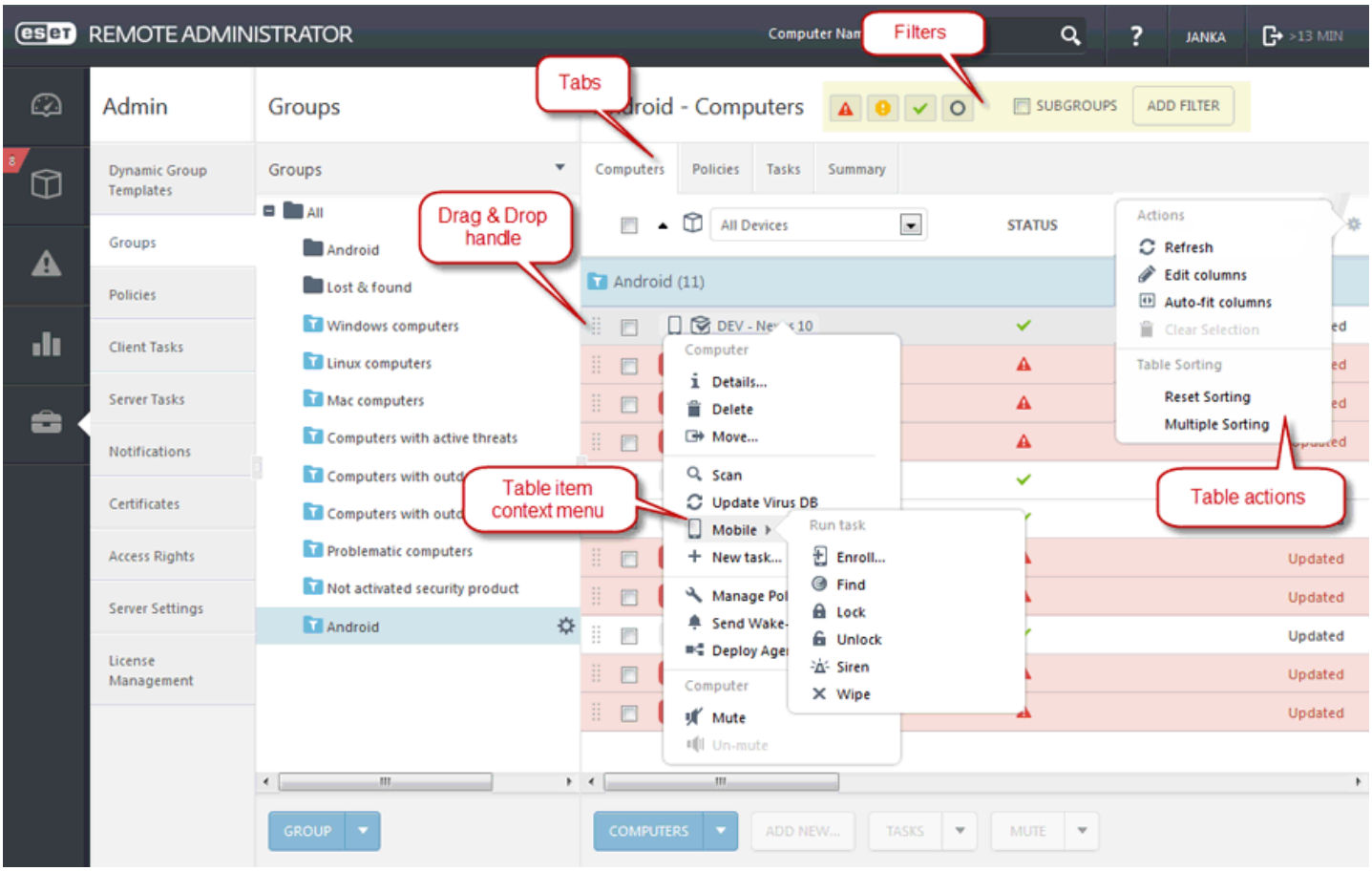
- The current user is always shown in upper right, where the timeout for his/her session counts down. You can click **Logout** next to the countdown to log out at any time. As soon as a session times out (because of user inactivity), a user must log in again.
- You can click **?** at the top of any screen to view **Screen help** for that specific screen.
- The **Menu** is accessible on the left at all times except when using a Wizard. Place your mouse on the left side of the screen to display the menu at any time. The menu also contains **Quick Links** and displays your **Web Console version.**
- The Cogwheel icon always denotes a context menu.



Screens with tree have specific controls. The tree itself is on the left with actions bellow. Click an item from the tree to display options for that item.

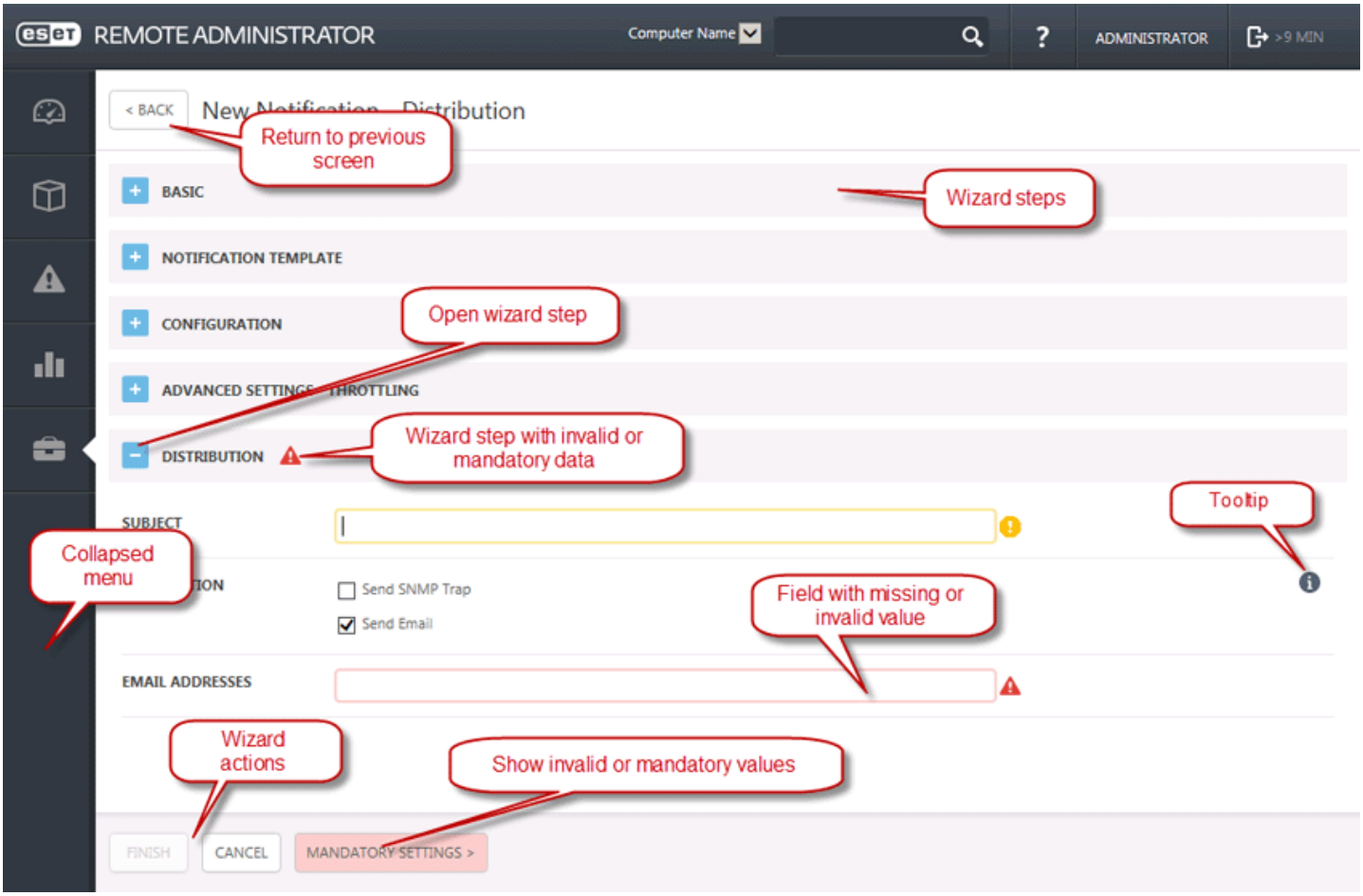


Tables allow you to manage units from rows individually or in a group (when more rows are selected). Click a row to display options for units in that row. Data in tables can be filtered and sorted.



Objects in ERA can be edited using Wizards. All Wizards share some common behavior:

- Steps are vertically oriented from top to bottom.
- User can return to any step at any time.
- Invalid input data are marked when you move your cursor to a new field. The Wizard step containing invalid input data is marked as well.
- User can check for invalid data any time by clicking **Mandatory Settings**.
- **Finish** is not available until all input data is correct.



4.4 Deployment

After the successful installation of ESET Remote Administrator, it is necessary to deploy the **ERA Agent** and **ESET Endpoint protection (EES, EEA...)** to the computers in the network. Deployment consists of following steps:

1. Add client computers to ESET Remote Administrator groups structure.
2. ERA Agent deployment
3. ESET Endpoint protection deployment

Once the ERA Agent is deployed, you can perform remote installation of other ESET security products on your client computers. The exact steps for remote installation are described in the Product installation chapter.

4.4.1 Add client computer to ERA structure

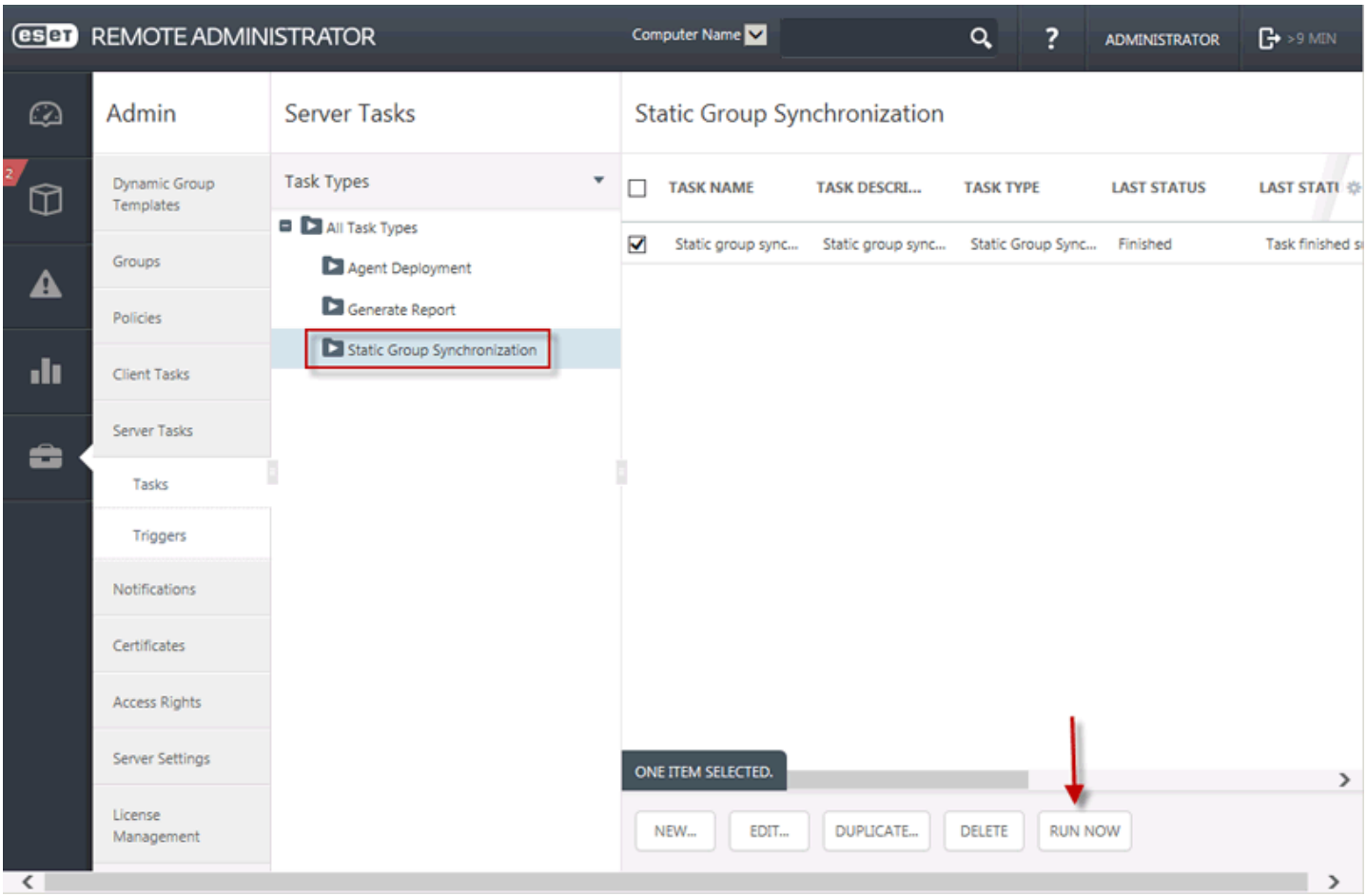
There are 3 ways to add client computer to ESET Remote Administrator:

- Active Directory synchronization
- Manually typing name/IP
- Using RD Sensor

4.4.1.1 Using Active Directory synchronization

AD synchronization is performed by running the **Static Group Synchronization** server task.

Admin > **Server Task** is a pre-defined default task that you can choose to execute automatically during ESET Remote Administrator installation. If the computer is in a domain, synchronization will be performed and computers from the AD will be listed in a default group **All**.

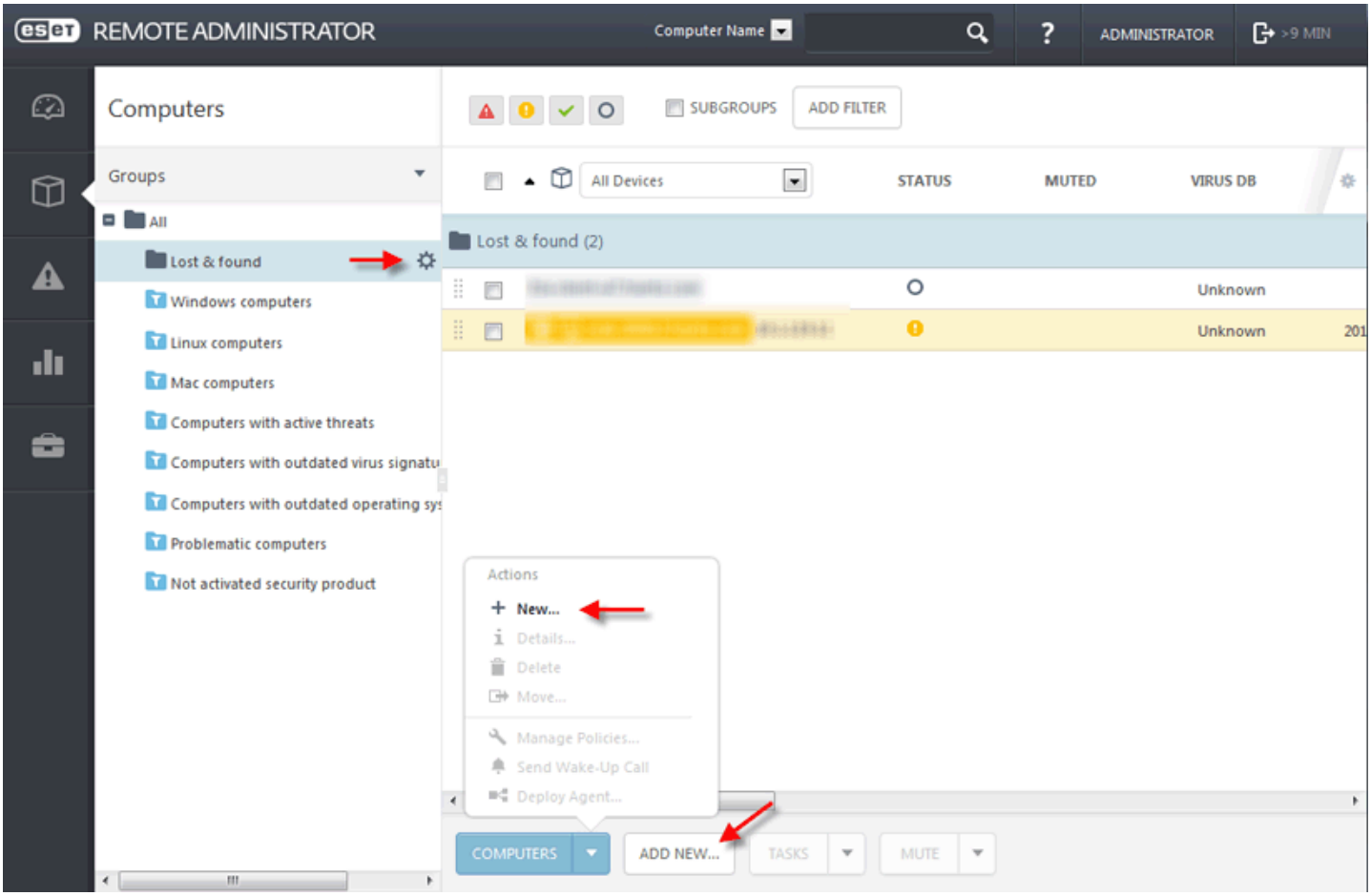


To start the synchronization process just click the task and choose **Run now**. If you need to create a new AD synchronization task, select a group to which you want to add new computers from the AD. Also select objects in the AD you want to synchronize from and what to do with duplicates. Enter your AD server connection settings and set the **Synchronization mode** to **Active Directory/Open Directory/LDAP**.

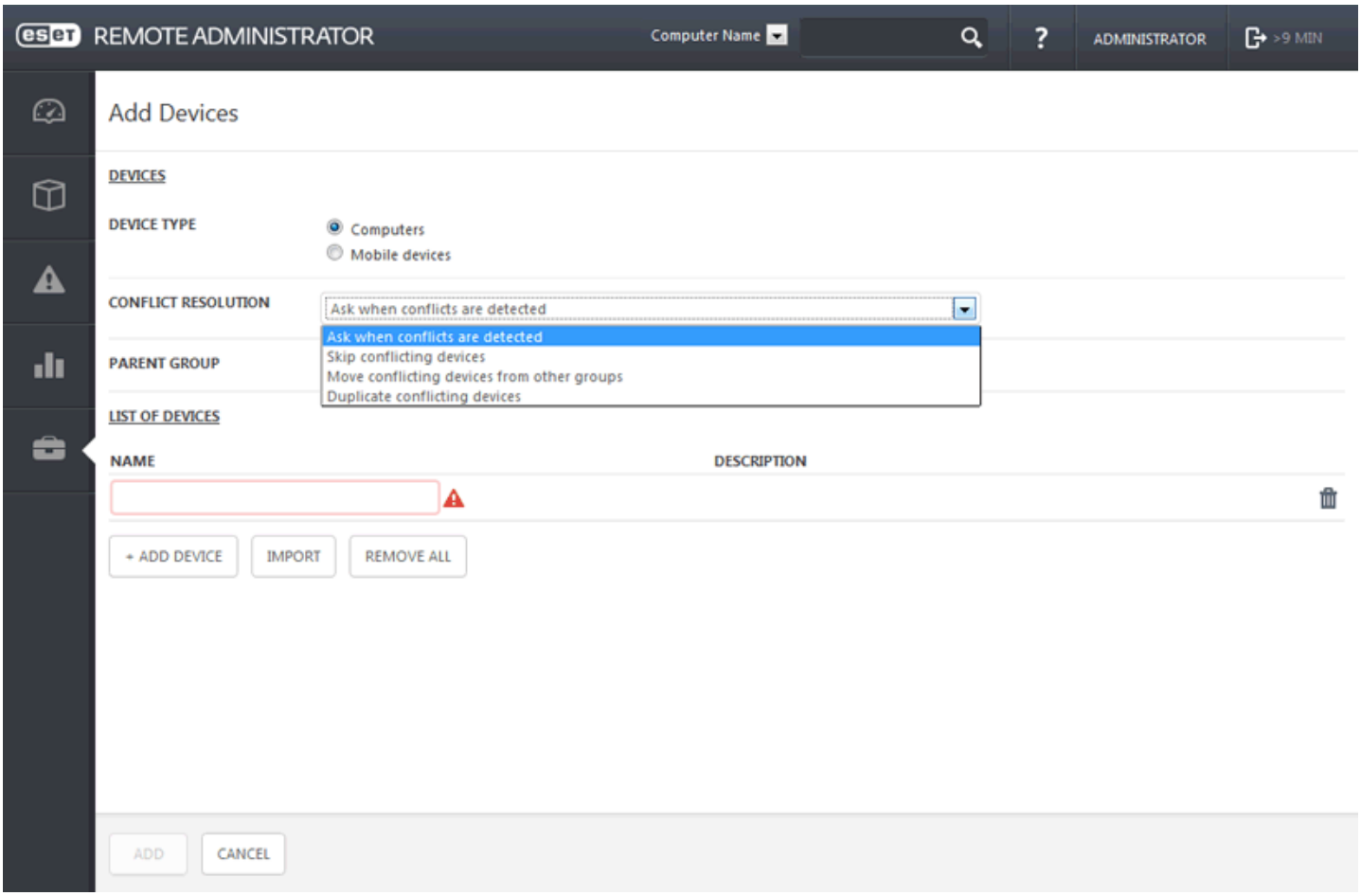
Follow step-by-step instructions in this ESET Knowledgebase article.

4.4.1.2 Manually typing name/IP

The **Computers** tab allows you to **Add New** computers. This way, you can manually Add computers that are not found or added automatically.



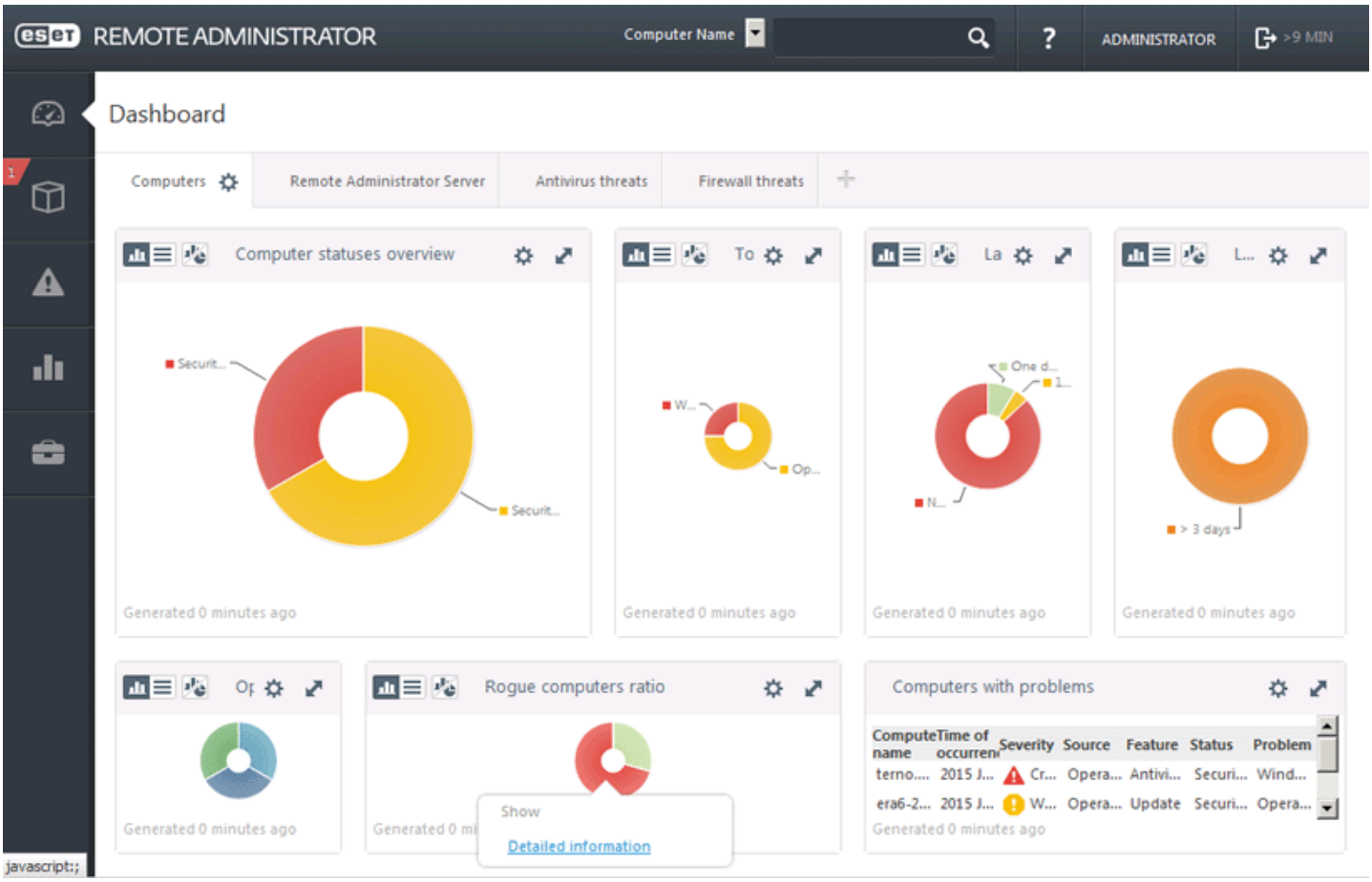
Type the **IP address** or **host name** of a machine you want to add and ESET Remote Administrator will search for it on the network.



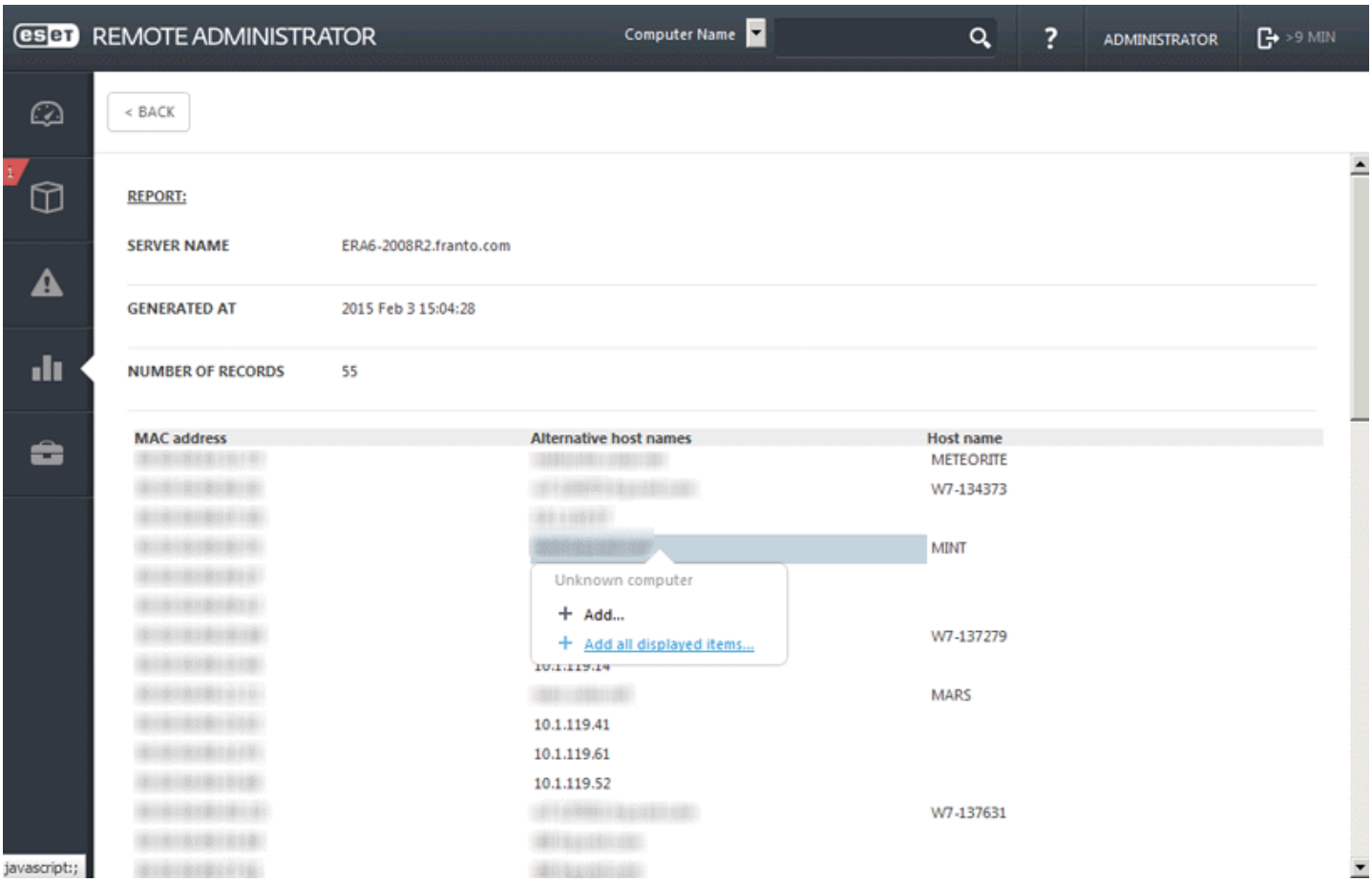
Click **Add**. Computers can be viewed in the list on the right when you select the group they belong to. Once the computer is added, a pop-up window will open with the option to **Deploy Agent**.

4.4.1.3 Using RD Sensor

If you are not using AD synchronization, the easiest way to add a computer into the ERA structure is to use **RD Sensor**. The RD sensor component is part of the installation bundle. You can easily drill down the report **Rogue computers ratio**, chart at the bottom of the Computers dashboard to view the rogue computers by clicking the red part of the graph.

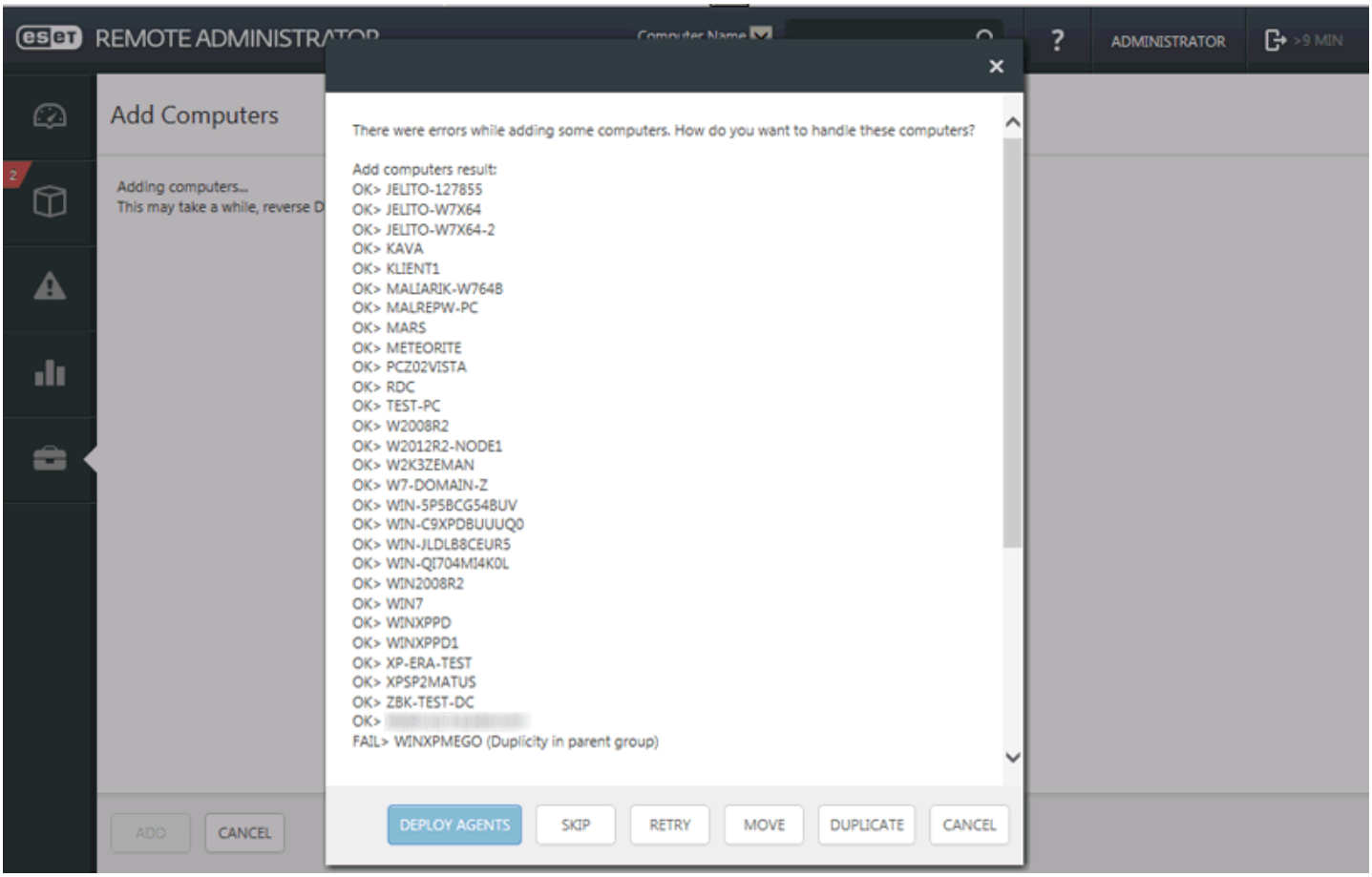


The **Rogue computers** report on the Dashboard now lists computers found by the RD Sensor. Computers can be added by clicking the computer you want to **Add**, or you can **Add all displayed items**.



If you are adding a single computer, follow the instructions on screen. You can use a preset name or specify your own (this is a display name that will be used in ERA Web Console only, not an actual host name). You can also add a description if you want to. If this computer already exists in your ERA directory, you will be notified and can decide what to do with the duplicate. The available options are: **Deploy Agent**, **Skip**, **Retry**, **Move**, **Duplicate** or **Cancel**. Once the computer is added, a pop-up window will open with an option to **Deploy Agent**.

If you click **Add all displayed items** a list of computers to be added will be displayed. Click **X** next to the name of a specific computer if you do not want to include it in your ERA directory at this time. When you are finished removing computers from the list, click **Add**. After clicking **Add**, select the action to take when a duplicate is found (allow for a slight delay depending on the number of computers in your list): **Skip**, **Retry**, **Move**, **Duplicate** or **Cancel**. Once you have selected an option, a pop-up window listing all added computers will open with an option to **Deploy Agents** on those computers.



The results of the RD Sensor scan are written to a log file called `detectedMachines.log`. It contains a list of discovered computers on your network. You can find the `detectedMachines.log` file here:

- Windows
  C:\ProgramData\ESET\Rouge Detection Sensor\Logs
- Linux
  var/log/eset/RemoteAdministrator/RogueDetectionSensor/detectedMachines.log

4.4.2 Agent deployment

Agent deployment can be performed in a few different ways. You can deploy the Agent:

Remotely - using a Server task for mass deployment of the ERA Agent, alternatively you can deploy the Agent using GPO and SCCM
Locally - using an Agent installation package or Agent Live Installers, for example, if problems occur during remote deployment

Local deployment can be performed in three ways:

- Agent Live Installers - using a generated script from within the ERA Web Console, you can distribute Agent Live Installers via email or run them from removable media (USB flash drive, etc.)
- Server assisted installation - using the Agent installation package downloads certificates from the ERA Server automatically (recommended local deployment method)
- Offline installation - using the Agent installation package, you must manually export certificates and use them in this deployment method

The Remote Agent deployment server task can be used for mass distribution of the Agent to client computers. It is the most convenient distribution method since it can be performed from Web Console without the need to deploy the Agent to each computer manually.

ERA Agent is very important because ESET security solutions running on client computers communicate with ERA Server exclusively through the Agent.

NOTE: Should you experience problems when deploying the ERA Agent remotely (the Server task **Agent deployment** fails) see the Troubleshooting guide.

4.4.2.1 Deployment steps - Windows

1. Make sure all **prerequisites** are met:

- **ERA Server** and the **ERA Web Console** are installed (on a Server computer).
- An Agent certificate is created and prepared on your local drive.
- A Certificate Authority is prepared on your local drive.
- The **Server computer** must be accessible from the network.

NOTE: Should you experience problems when deploying ERA Agent remotely - the Server task **Agent deployment** ends with status Failed - see the Troubleshooting guide.

2. Double-click the installation package to begin installation.
3. Enter a **Server host** (hostname/ip address) and a **Server port** (by default 2222) in the appropriate fields. These are used for connection to the ERA Server.
4. Select a peer certificate and a password for this certificate. Optionally, you can add a certificate authority. This is only required for unsigned certificates.
5. Select a folder where the **Agent** will be installed, or leave the pre-defined folder selected.
6. Click **Install**. The **Agent** will be installed on your computer.

NOTE: If a detailed log from the installation is required, the user must start the installation through the *msiexec* program, and supply the needed parameters: `msiexec /i program_installer.msi /lv* c:\temp\installer_log.txt`

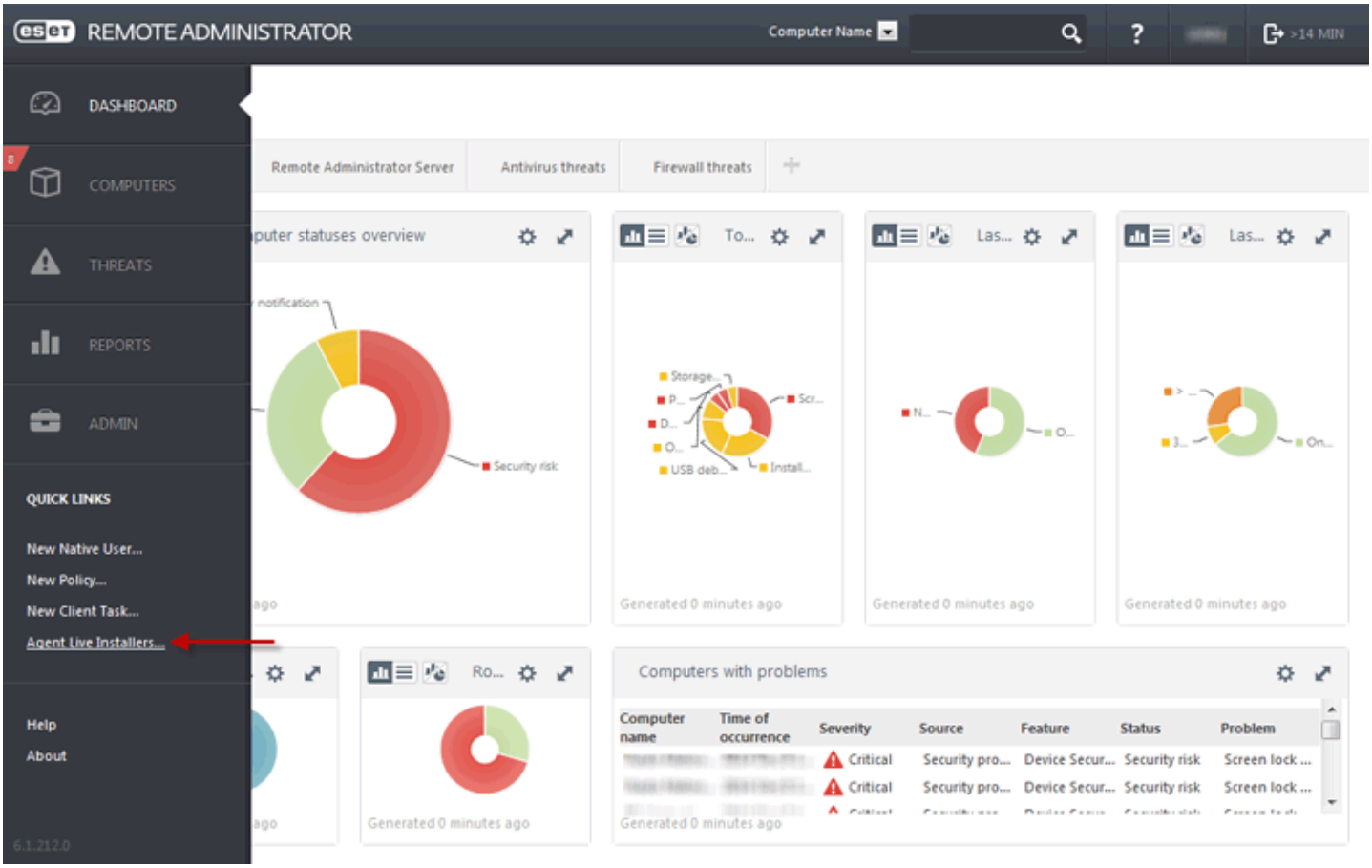
- The folder *c:\temp* must exist prior to executing this command.
- You can check the status log on the client machine *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* to make sure ERA Agent is working properly.

4.4.2.1.1 Agent Live Installers

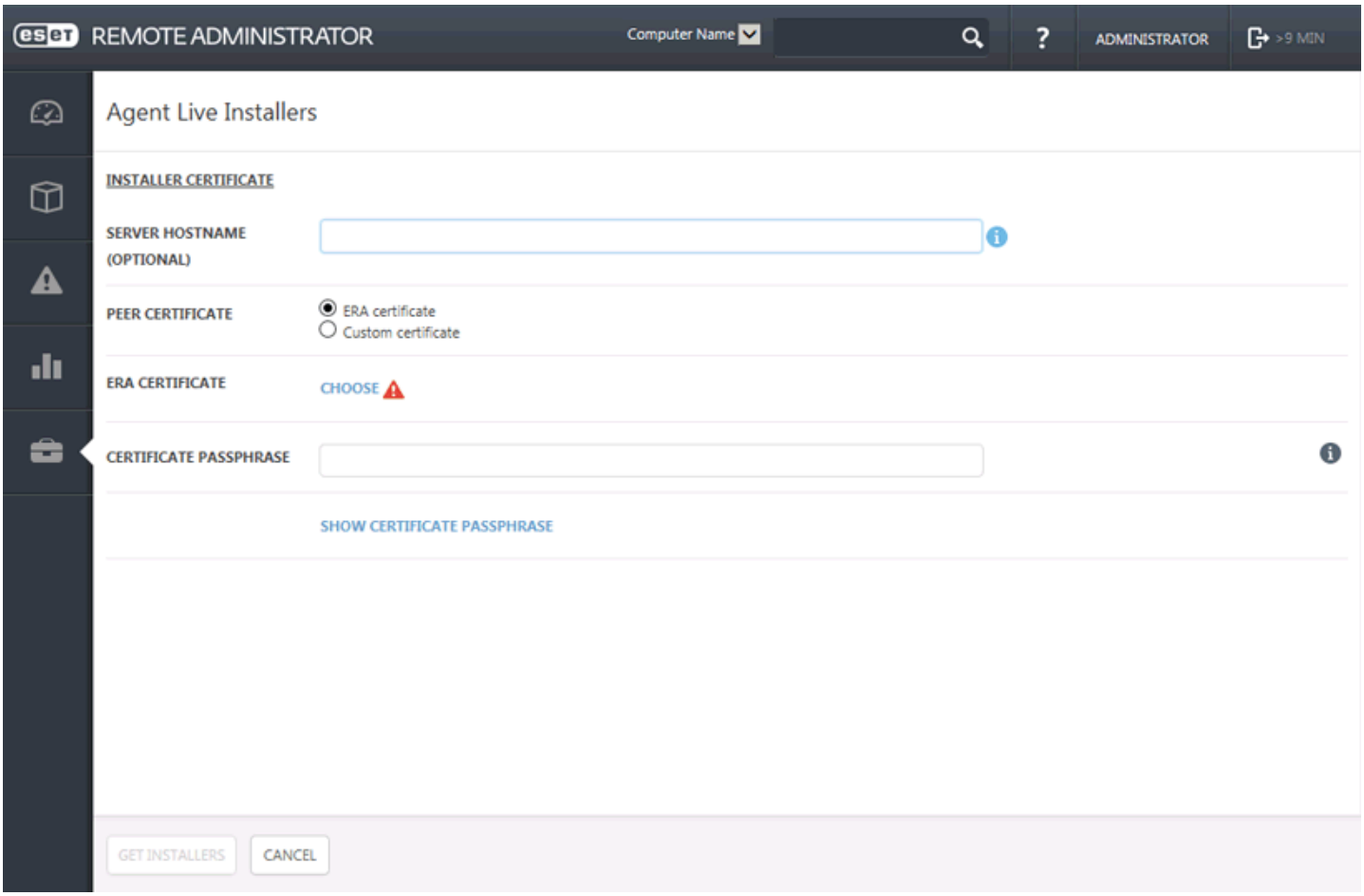
This type of Agent deployment is useful when the remote and local deployment options do not suit you. In such cases, you can distribute the Agent Live Installer via email and let the user deploy it. You can also run the Agent Live Installer from removable media (USB flash drive, etc.).

NOTE: The client machine needs to have an internet connection to download the Agent installation package. Also, the client needs to be able to connect to the ERA Server.

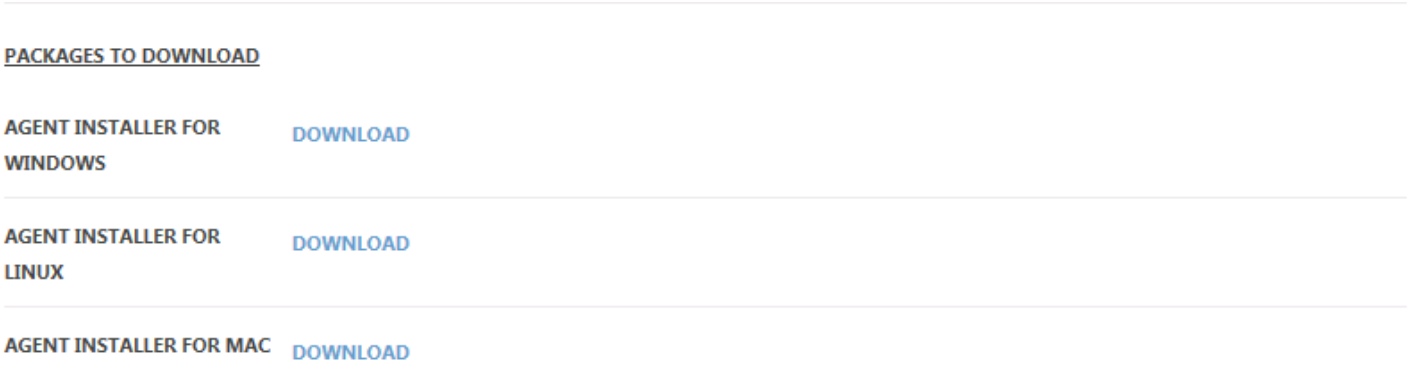
1. Click **Agent Live Installers...** in the **Quick Links** section of the menu bar to create the installer.



2. Enter the server hostname or IP address and select the **ERA Certificate Authority** that you created during initial installation. Enter the **Certification authority passphrase** that you created during **Server Installation** when prompted for the certificate password.



3. Click **Get Installers** to generate links for Windows, Linux and MAC Agent installer files.



4. Click the **Download** link next to the installer file(s) that you want to download and save the **zip** file. Unzip the file on the client computer where you want to deploy ERA Agent and run `EraAgentOnlineInstaller.bat` (Windows) or `EraAgentOnlineInstaller.sh` script (Linux and Mac) to run the installer.

NOTE: If you are running the script on Windows XP SP2, you need to install Microsoft Windows Server 2003 Administration Tools Pack. Otherwise, the Agent Live Installer won't run properly. Once you have installed the Administration Pack, you can run the Agent Live Installer script.

You can check the status log on the client machine *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* to make sure ERA Agent is working properly. If there are problems with the Agent (for example, it is not connecting to the ERA Server) see troubleshooting.

If you want to deploy ERA Agent using Agent Live Installer from your local shared folder without ESET Repository Download Server, follow these steps:

1. Edit the `EraAgentOnlineInstaller.bat` file (Windows) or `EraAgentOnlineInstaller.sh` script (Linux and Mac).
2. Change lines 28 and 30 to point to the correct local download files. For example:

```
27
28  set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x64.msi
29  if defined IsArch_x86 (
30    set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x86.msi
31  )
```

3. Use your own URL (instead of the one shown below):

```
26  )
27
28  set url=\\server\share\Agent_x86.msi
29  if defined IsArch_x86 (
30    set url=\\server\share\Agent_x86.msi
31  )
```

4. Edit line 80 to replace " **^& packageLocation ^&** "

```
79  echo.
80  echo.Dim params: params = "/qr /i " ^& packageLocation ^& " /l*v %temp%\ra-agent-install.log" ^&_
```

with **!url!**

```
79  echo.
80  echo.Dim params: params = "/qr /i !url! /l*v %temp%\ra-agent-install.log" ^&_
```

5. **Save** the file.

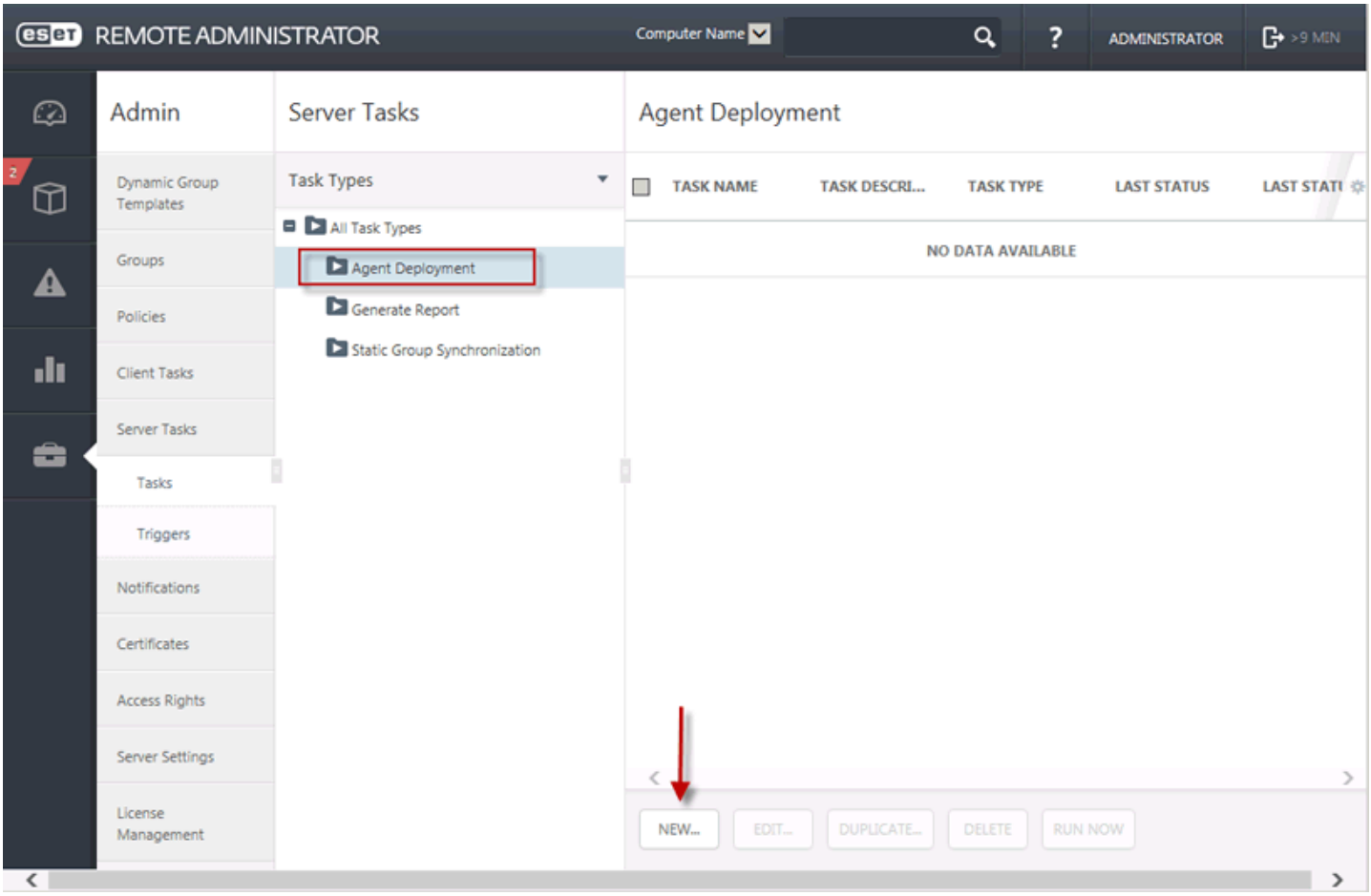
4.4.2.1.2 Deploy Agent remotely

There are two options for remote deployment of the ERA Agent. You can use a Server task as described below or you can deploy the Agent using GPO and SCCM.

Remote deployment of the ERA Agent using a Server task is performed from the **Admin** section. Use the following written instructions or watch our Knowledgebase instructional video.

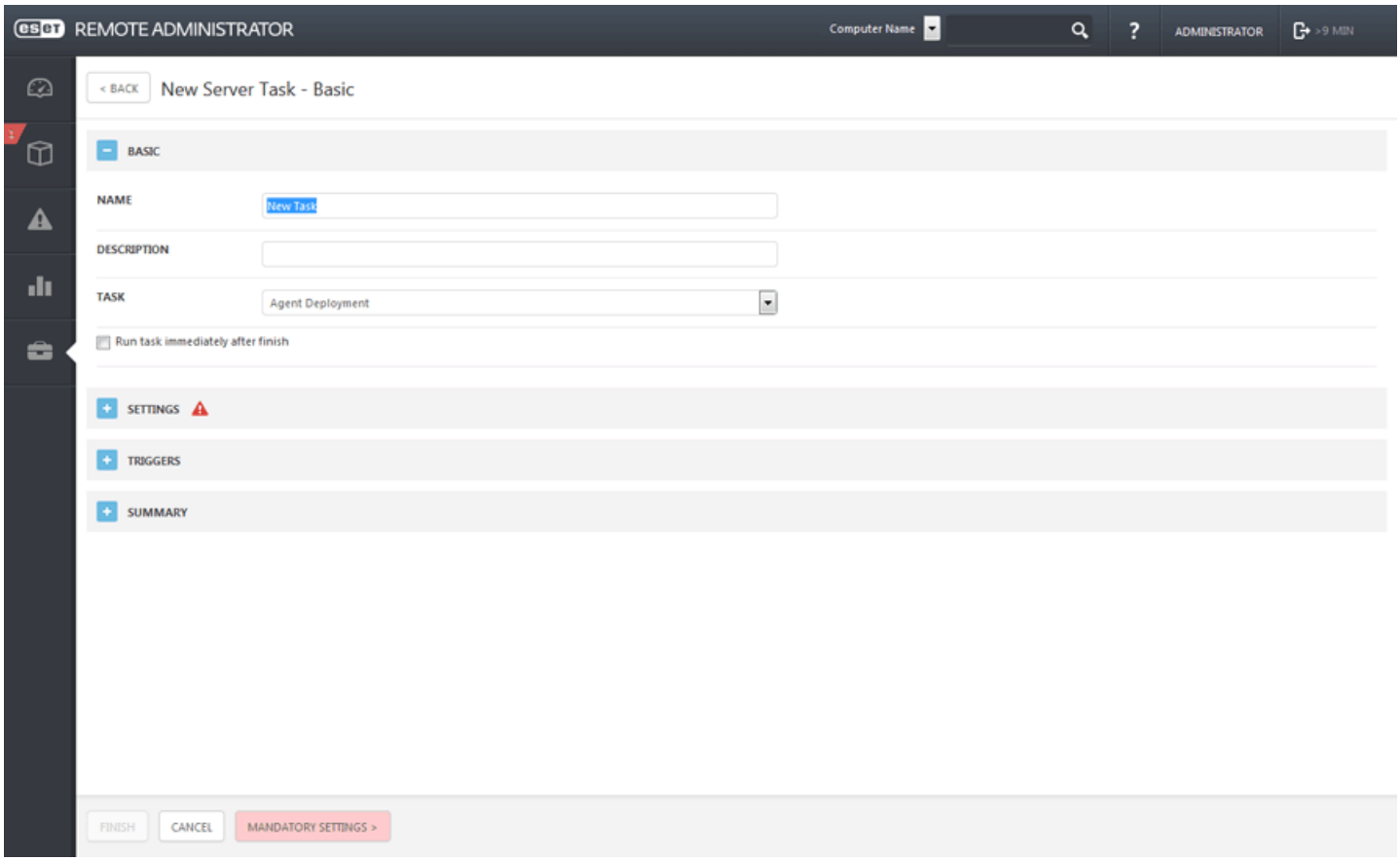
NOTE: We recommend that you test mass Agent deployment in your environment before using it to deploy the ERA Agent to large groups of clients. Before testing mass deployment, set the Agent connection interval to your preference.

Click **Server Task** > **Agent Deployment** > **New** to start configuring your new task.



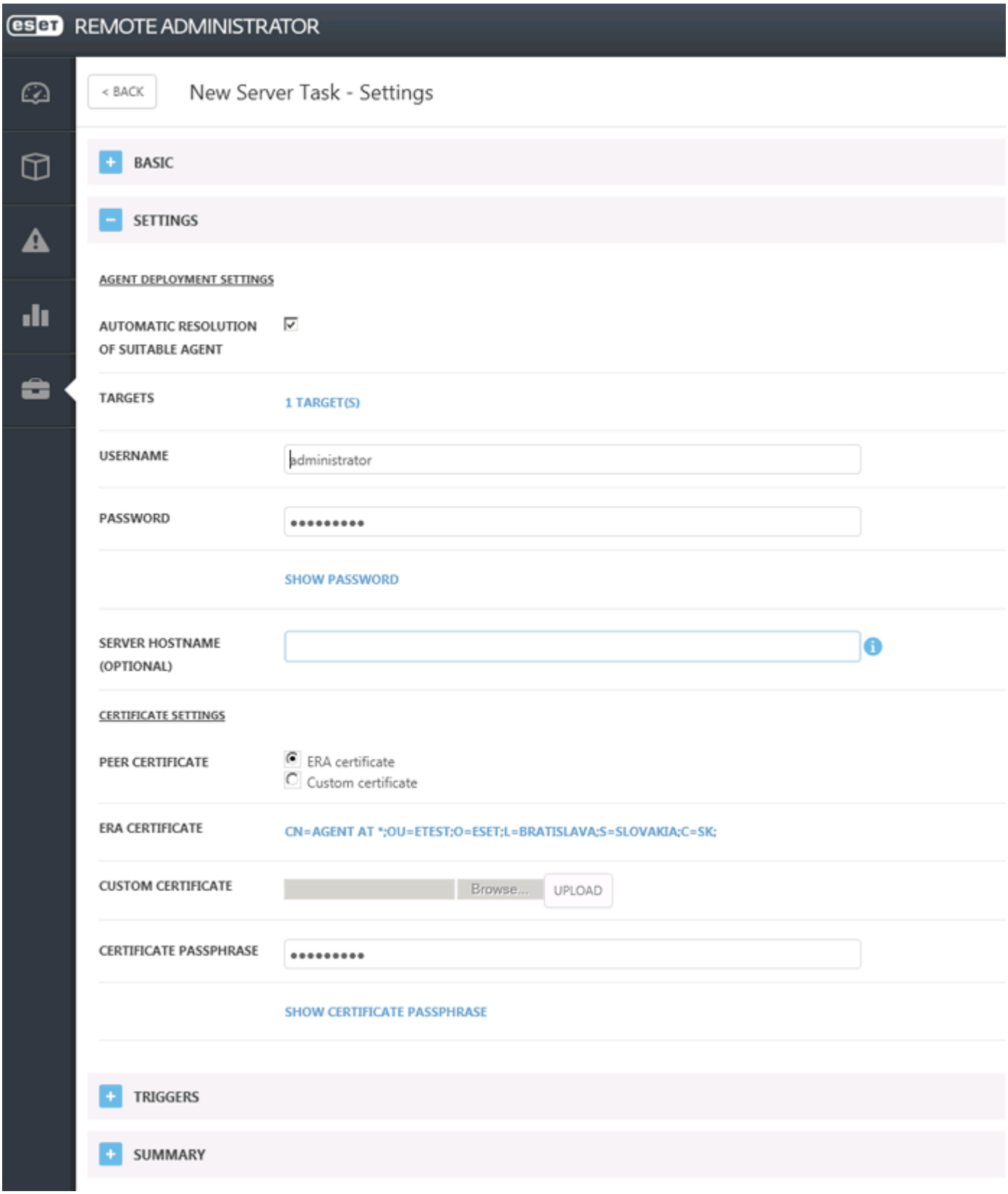
Basic

Enter basic information about the task, such as the **Name**, **Description** (optional) and **Task Type**. The **Task Type** defines the settings and behavior of the task.



Settings

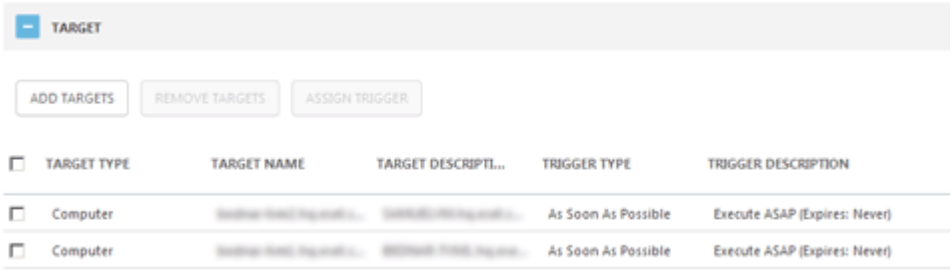
- **Automatic resolution of suitable Agent** - If you have multiple operating systems (Windows, Linux, Mac OS) in your network, select this option and this task will automatically find the appropriate server-compatible Agent installation package for each system.
- **Targets** - Click this to select the clients that will be the recipients of this task.
- **Username/Password** - The username and the password for the user with sufficient rights to perform a remote installation of the agent.
- **Server hostname (optional)** - You can enter a server hostname if it is different on the client side and the server side.
- **Peer certificate/ERA Certificate** - This is the security certificate and certificate authority for the agent installation. You can select the default certificate and certificate authority, or use custom certificates. For more information, see the Certificates chapter.
- **Custom certificate** - If you use a custom certificate for authentication, navigate to the certificate and select it when installing the Agent.
- **Certificate passphrase** - Password for the certificate, either the password you entered during Server installation (in the step where you created a certificate authority) or the password for your custom certificate.



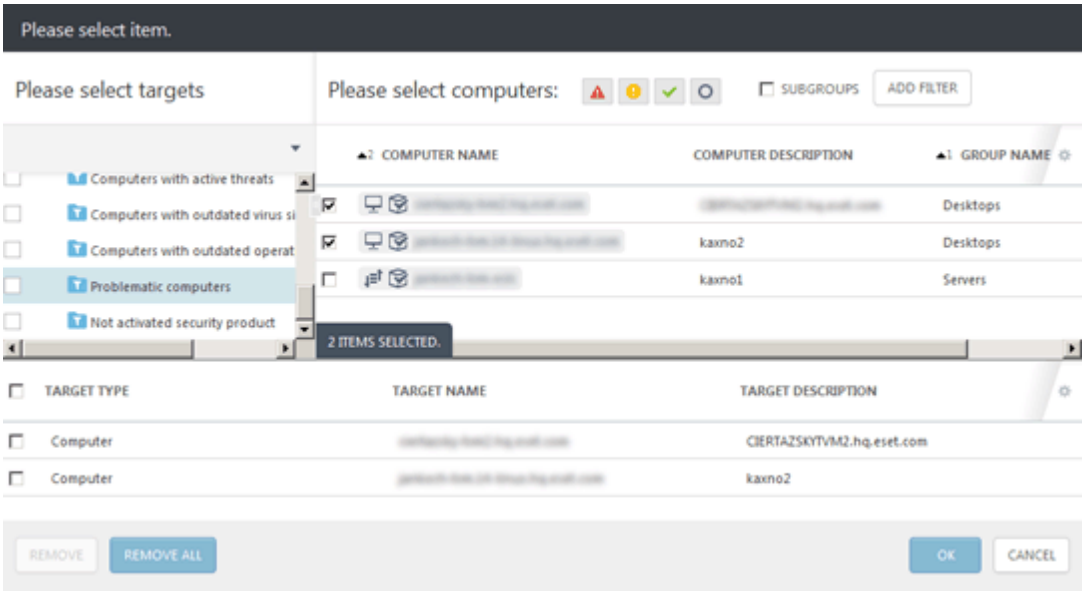
NOTE: ERA Server can select the appropriate Agent installation package for operating systems automatically. To choose a package manually, deselect **Automatic resolution of suitable Agent** and then choose the package you want to use from the list of available Agents in ERA repository.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

NOTE: Should you experience problems when deploying ERA Agent remotely (the Server task **Agent deployment** fails) see the Troubleshooting section of this guide.

4.4.2.1.3 Deploy Agent locally

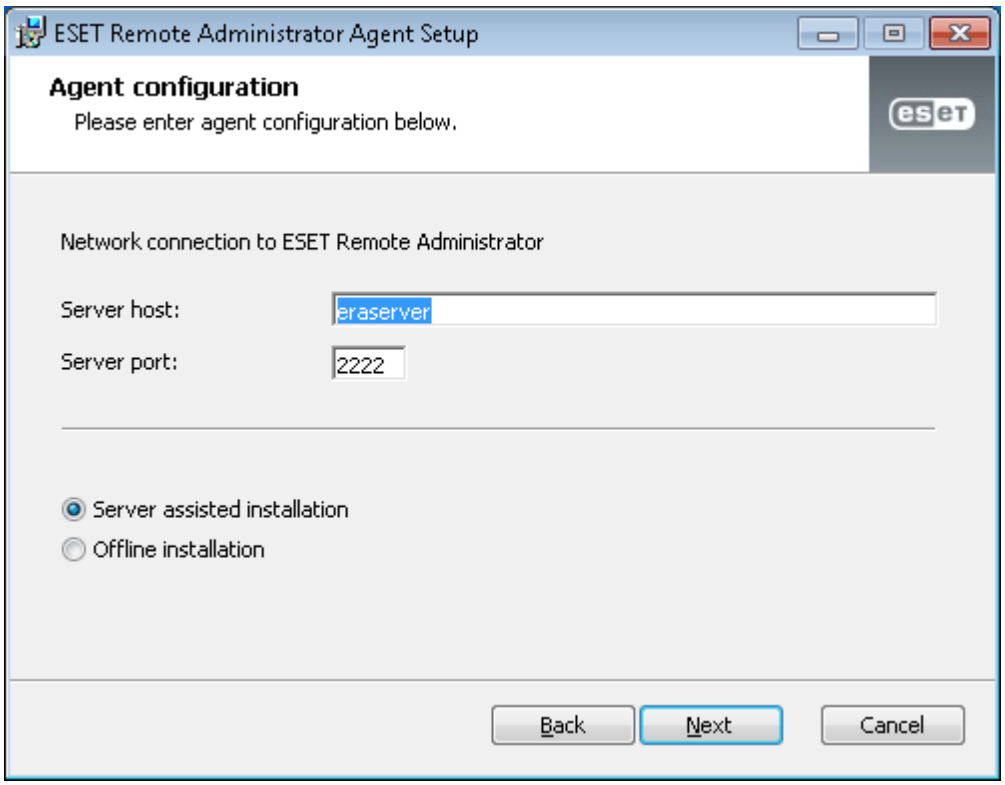
To deploy the Agent locally on a client computer using installation wizard, follow the steps below:

Download the Agent installation package from the download section of the ESET website under **Remote Management** (click the + sign to expand the category). Run the installer on client machine you want to deploy the Agent to. After accepting the EULA, select the type of installation you want to perform - Server assisted installation or Offline installation.

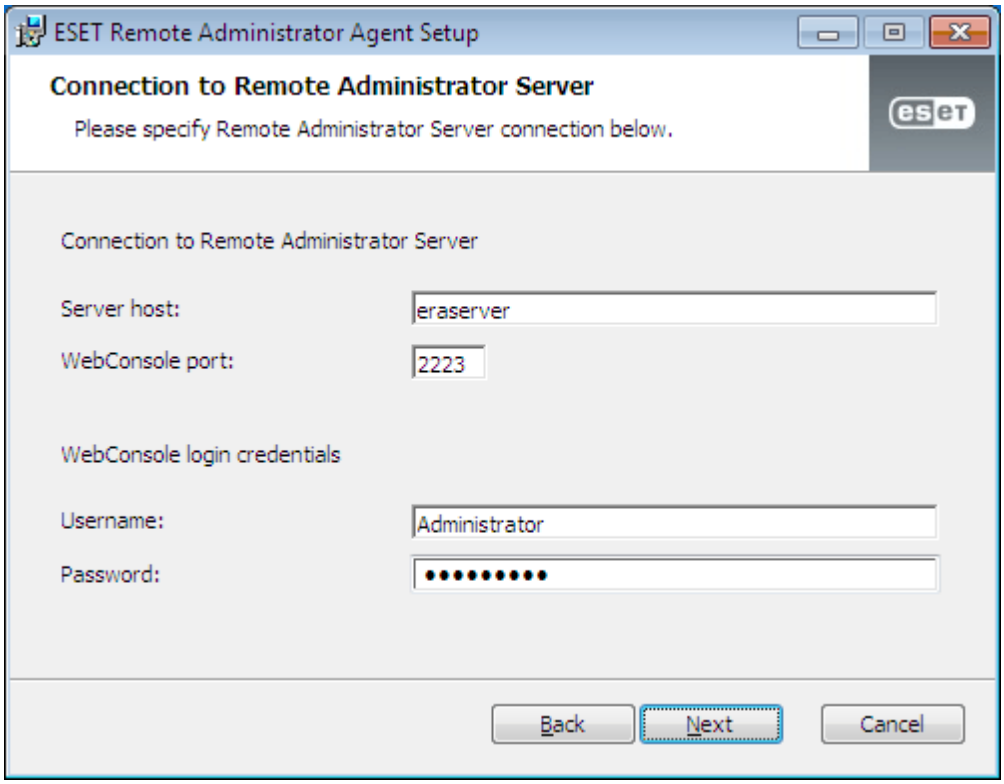
Use following written instructions or watch Knowledgebase instructional video. Also, you can use this ESET Knowledgebase article with illustrated step-by-step instructions.

1. **Server assisted installation**:

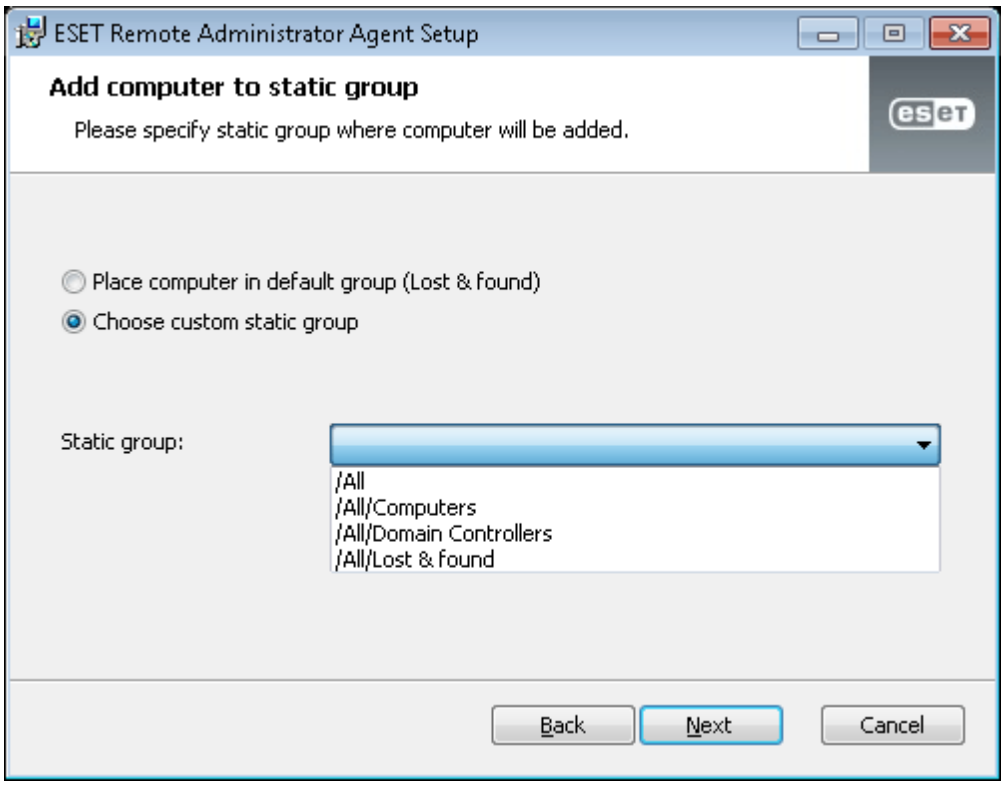
Make sure **Server assisted installation** is selected, specify your **Server host** (name or IP address) and the **Server port** of your ERA Server and then click **Next**. The default Server port is 2222, if you are using a different port, replace the default port with your custom port number.



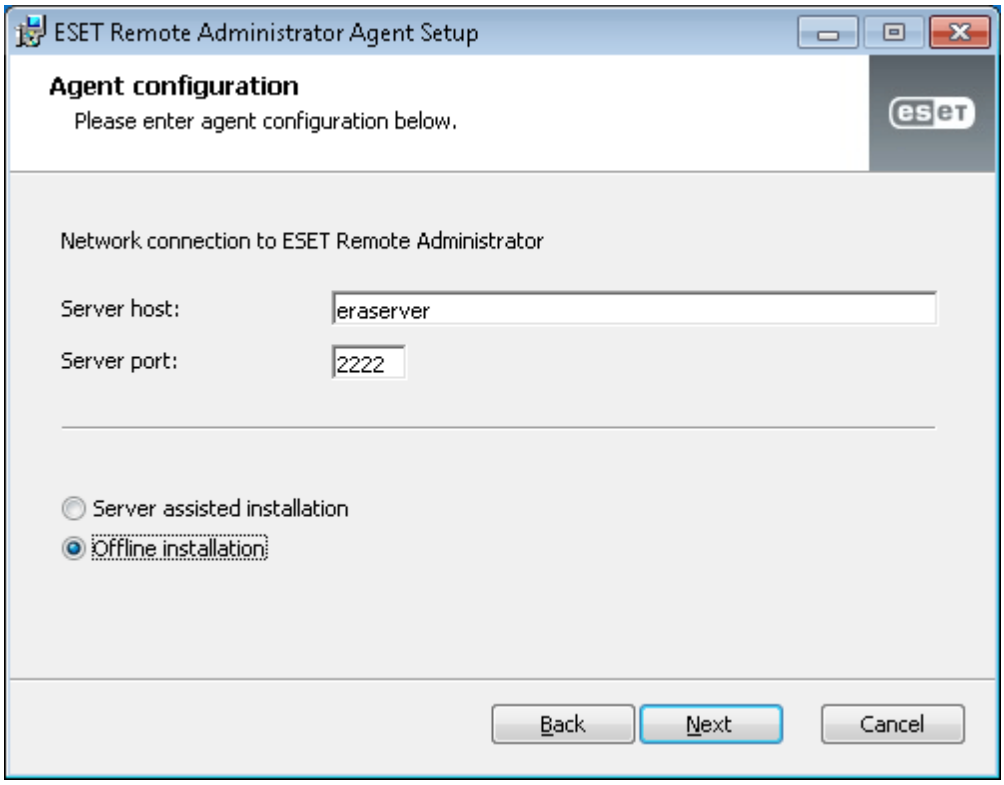
Specify the method used for connection to Remote Administrator Server: **ERA Server** or **ERA Proxy Server** and ERA Web Console port and enter your ERA Web Console login credentials: **Username** and **Password**.



Click **Choose custom Static Group** and select the Static Group to which the client computer will be added using the drop-down menu.

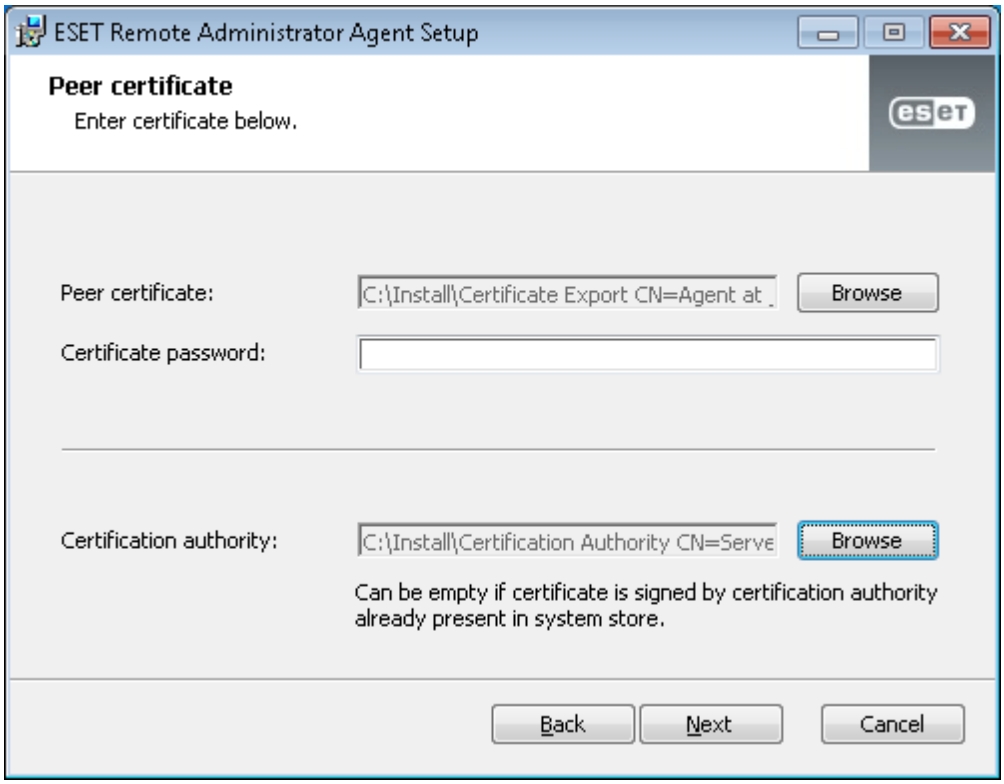


2. **Offline installation**:



To perform an **Offline installation**, enter **2222** in the **Server port** field, select **Offline installation** and click **Next**. For this method you must specify a **Peer certificate** and **Certification Authority**.

For more information about how to export and use a **Peer certificate** and **Certification Authority** click here.



NOTE: You can check the status log on a client machine (located at *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html)* to make sure the ERA Agent is working properly. If there are problems with the Agent (for example, if it is not connecting to the ERA Server) see troubleshooting.

4.4.2.2 Deployment steps - Linux

These steps apply when performing a local installation of the Agent. If you want to deploy the Agent on multiple computers, see the Agent Deployment section.

Make sure the following prerequisites are met:

- ERA Server and the ERA Web Console installed (on a Server computer).
- An Agent certificate created and prepared on your local drive.
- Certificate Authority prepared on your local drive.
- The **Server computer** must be accessible from the network.
- The Agent installation file must be set as an executable (chmod +x).

The Agent is installed by running a command in the terminal (see the example below).

Example
(New lines are denoted by "\" to make it easier to copy this string into Terminal)

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/adminko/Desktop/agent.pfx \
--cert-auth-path=/home/adminko/Desktop/CA.der --cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 --port=2222
```

ERA Agent and the eraagent.service will be installed in the following location:
/opt/eset/RemoteAdministrator/Agent

Installation parameters

- *--skip-license* will not ask the user for license confirmation.
- *--cert-path* is the path to Agent certificate file.
- *--cert-auth-path* is the path to the Server certification authority file.
- *--cert-password* must match the Agent certificate password
- *--hostname* is an connection to the server (or proxy) in one of these formats (hostname, IPv4, IPv6 or SRV record)
- *--port* is a port for listening, both for the Server and the Proxy (2222).

To verify a correct installation, run the following command:

```
sudo service eraagent status
```

NOTE: When you use a certificate that you created, signed by an authority other than the ERA Certificate Authority, it is necessary to leave the parameter *--cert-auth-path* out of the installation script, because the other Certification Authority is already installed on your Linux OS (and also on your Server computer).

NOTE: Should you experience problems when deploying ERA Agent remotely (the Server task **Agent deployment** ends with a Failed status) see the Troubleshooting guide.

You can check the status log on the client machine */var/log/eset/RemoteAdministrator/Agent/trace.log* or */var/log/eset/RemoteAdministrator/Agent/status.html* to make sure ERA Agent is working properly.

4.4.2.3 Deployment steps - OS X

1. Make sure all **prerequisites** are met:

- **ERA Server** and the **ERA Web Console** are installed (on a Server computer).
- An Agent certificate is created and prepared on your local drive.
- A Certificate Authority is prepared on your local drive.

NOTE: Should you experience problems when deploying ERA Agent remotely (the Server task **Agent deployment** ends with a Failed status) see the Troubleshooting guide.

2. Double click the *.dmg* file to start installation.

3. Enter the **Server connection** data: **Server host** (hostname or IP address of the ERA Server) and the **Server port** (by default 2222).

4. Select a peer certificate and a password for this certificate. Optionally, you can add a certificate authority. This is only needed for unsigned certificates.

5. Review the install location and click **Install**. The **Agent** will be installed on your computer.

6. The ERA Agent log file can be found here: */Library/Application Support/com.eset.remoteadministrator.agent/Logs/*

4.4.2.4 Troubleshooting - Agent deployment

You may encounter problems with Agent deployment. If deployment fails, there are a number of things that might be the cause. This section will help you:

- Find out what caused Agent deployment to fail
- Check for possible causes according to the table below
- Resolve the issue and perform a successful deployment

Windows

1. To find out why Agent deployment failed, navigate to **Reports** > **Automation**, select **Agent Deployment task information in last 30 days and** click **Generate now**.
A table will displayed deployment information. The **Progress** column displays error messages about why Agent deployment failed.

If you need even more details, you can change the verbosity of the ERA Server trace log. Navigate to **Admin** > **Server Settings** > **Advanced Settings** > **Logging** and select **Error** from the drop-down menu. Run the Agent deployment again and when it fails check the ERA Server trace log file for the latest log entries at the bottom of the file. The report will include suggestions about how to resolve the issue. The latest ERA Server log file can be found here: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*

To enable full logging, create a dummy file named **traceAll** without an extension in the same folder as a trace.log. Restart the ESET Remote Administrator Server service, this will enable full logging into **trace.log** file.

2. The table below contains several reasons Agent deployment can fail:

Error message	Possible cause
Could not connect	Client is not reachable on the network Client's host name could not be resolved Firewall blocks communication Ports 2222 and 2223 are not open in firewall (on both client and server side)
Access denied	No password set for administrator account Insufficient access rights ADMIN$ administrative share is not available IPC$ administrative share is not available Use simple file sharing is enabled
Package not found in repository	Link to the repository is incorrect Repository is unavailable Repository doesn't contain required package

3. Follow the appropriate troubleshooting steps according to the possible cause:

- **Client is not reachable on the network** - ping the client from the ERA Server, if you get a response, try to log on to the client machine remotely (for example, via remote desktop).
- **Client's host name could not be resolved** - possible solutions to DNS issues can include but are not limited to:

  Using the `nslookup` command of the IP address and hostname of the server and/or the clients having Agent deployment issues. The results should match the information from the machine. For instance, an `nslookup` of a hostname should resolve to the IP address an `ipconfig` command shows on the host in question. The `nslookup` command will need to be run on the clients and the server.

  Manually examining DNS records for duplicates.

- **Firewall blocks communication** - check the firewall settings on both the server and the client, as well as any other firewall that exists between these two machines (if applicable).
- **Ports 2222 and 2223 are not open in firewall** - same as above, make sure that these ports are open on all firewalls between the two machines (client and server).
- **No password set for administrator account** - set a proper password for the administrator account (do not use a blank password)
- **Insufficient access rights** - try using the Domain Administrator's credentials when creating an Agent deployment task. If the client machine is in a Workgroup, use the local Administrator account on that particular machine.
- **ADMIN$ administrative share is not available** - The client machine must have the shared resource **ADMIN$** activated, make sure it is present among the other shares (**Start** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Shared Folders** > **Shares**).
- **IPC$ administrative share is not available** - verify that the client can access IPC by issuing the following from a command prompt on the client:

  ```
  net use \\servername\IPC$
  ```

  where *servername* is the name of the ERA Server
- **Use simple file sharing is enabled** - if you are getting the "Access denied" error message and your environment is mixed (contains both a Domain and Workgroup), disable **Use simple file sharing** or **Use Sharing Wizard** on all machines that are having problems with Agent deployment. For example, in Windows 7 do the following:
  - Click **Start**, type `folder` into the **Search** box, and then click **Folder Options**. Click the **View** tab and in the **Advanced settings** box, scroll down the list and deselect the check box next to **Use Sharing Wizard**.
- **Link to the repository is incorrect** - In ERA Web Console, navigate to **Admin** > **Server Settings,** click **Advanced settings** > **Repository** and make sure the URL of the repository is correct.
- **Package not found in repository** - this error message usually appears when there is no connection to the ERA repository. Check your Internet connection.

NOTE: For later Windows operating systems (Windows 7, Windows 8, etc.) the Administrator user account must be activated in order to run the Agent deployment task.

To activate the Administrator user account:

1. Open an administrative command prompt
2. Enter the following command: `net user administrator /active:yes`

Linux and Mac OS

If Agent deployment does not work on Linux or Mac OS, the issue is usually related to SSH. Check the client computer and make sure SSH daemon is running. Once fixed, run Agent deployment again.

4.4.3 Agent deployment using GPO and SCCM

After a successful installation of ESET Remote Administrator, it is necessary to deploy the **ERA Agent** and ESET security products to client computers in your network.

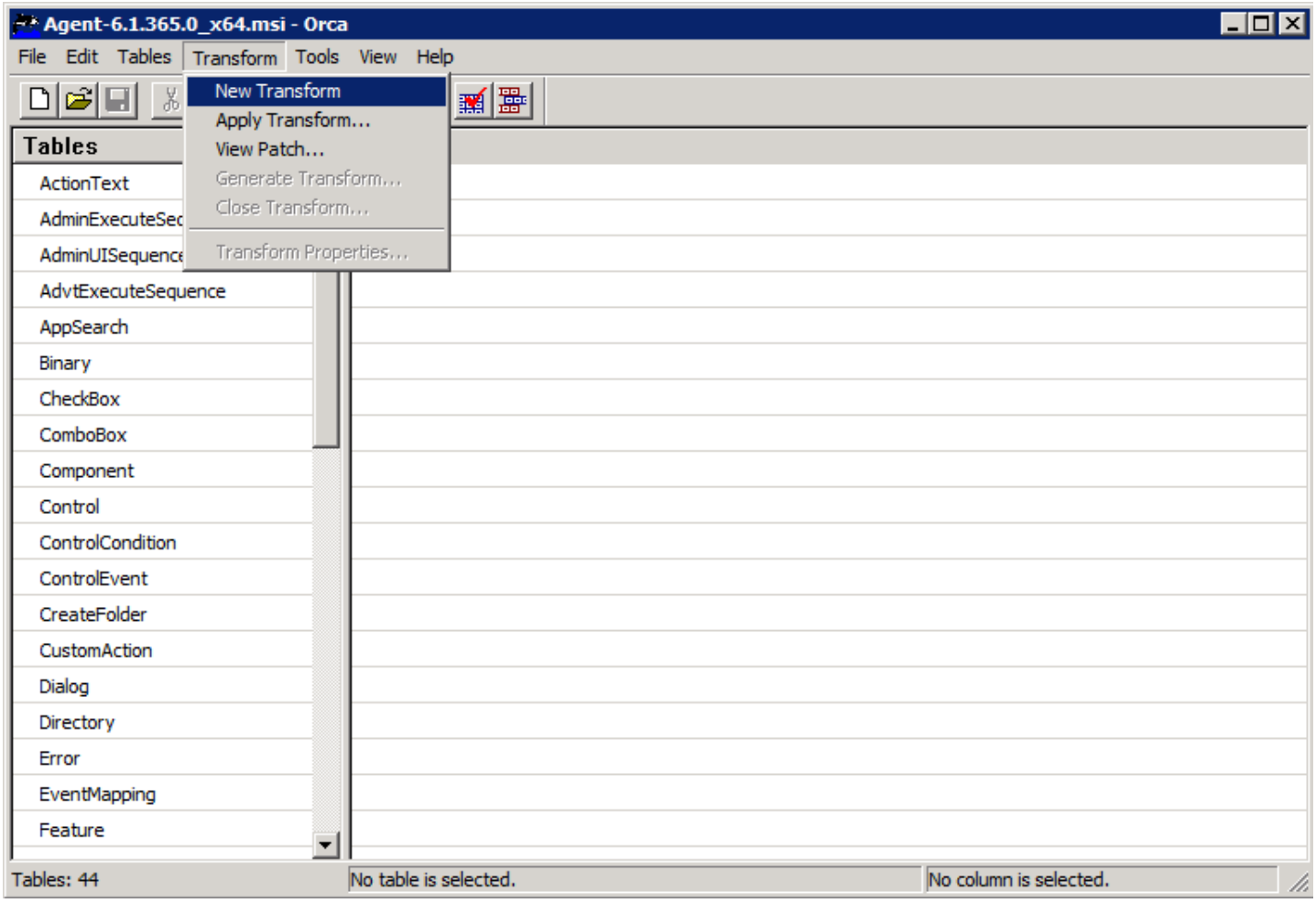
Apart from local deployment or remote deployment using a Server task, you can also you use management tools such as GPO, SCCM, Symantec Altiris or Puppet. CLick the appropriate link below to view step-by-step instructions for two popular ERA Agent deployment methods:

1. Deployment of ERA Agent using GPO
2. Deployment of ERA Agent using SCCM

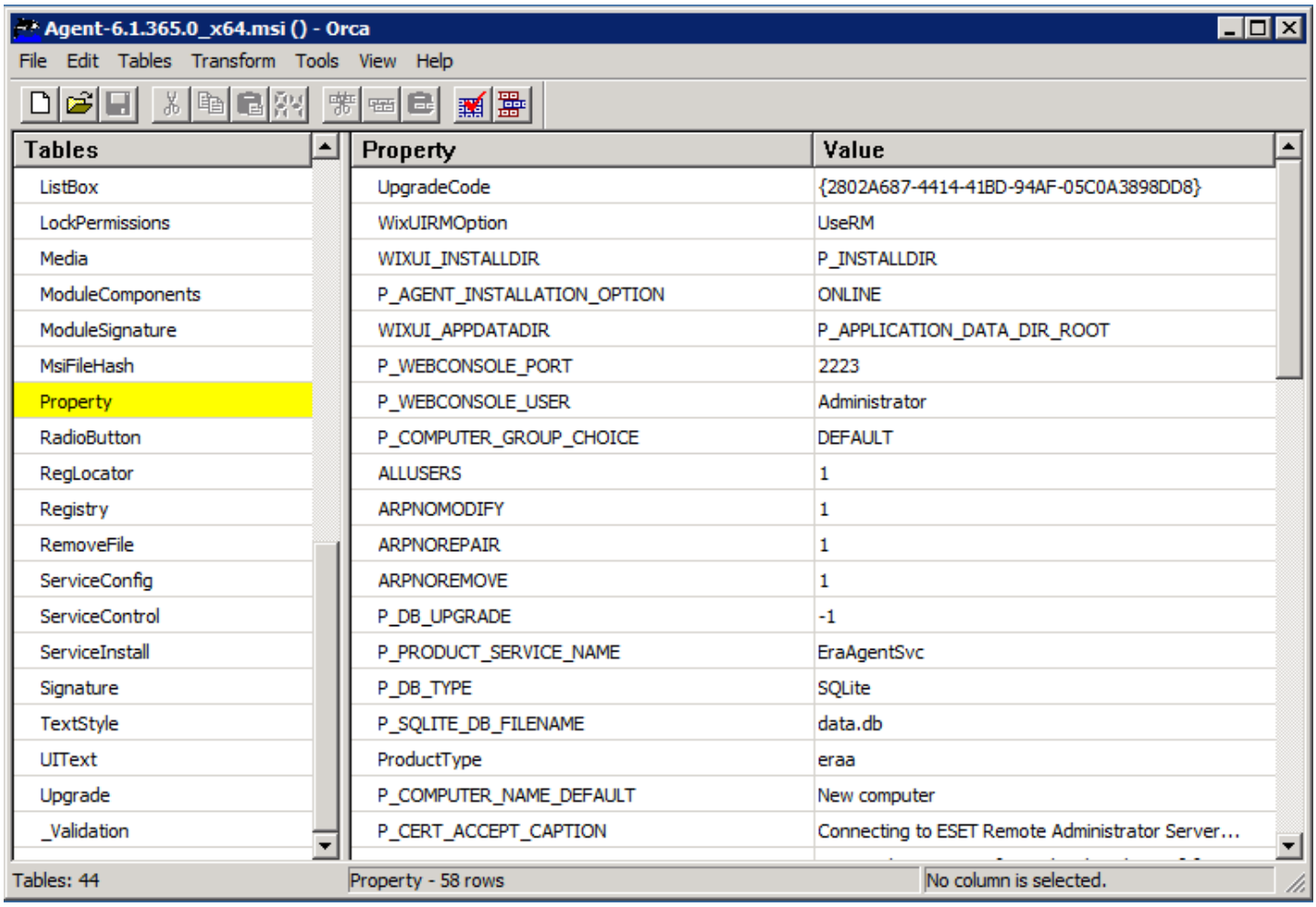
4.4.3.1 Creating MST file

Before you deploying the ERA Agent installer file, you need to create a transform `.mst` file with settings for ERA Agent. To create a transform file, follow the steps below or see our Knowledgebase article.

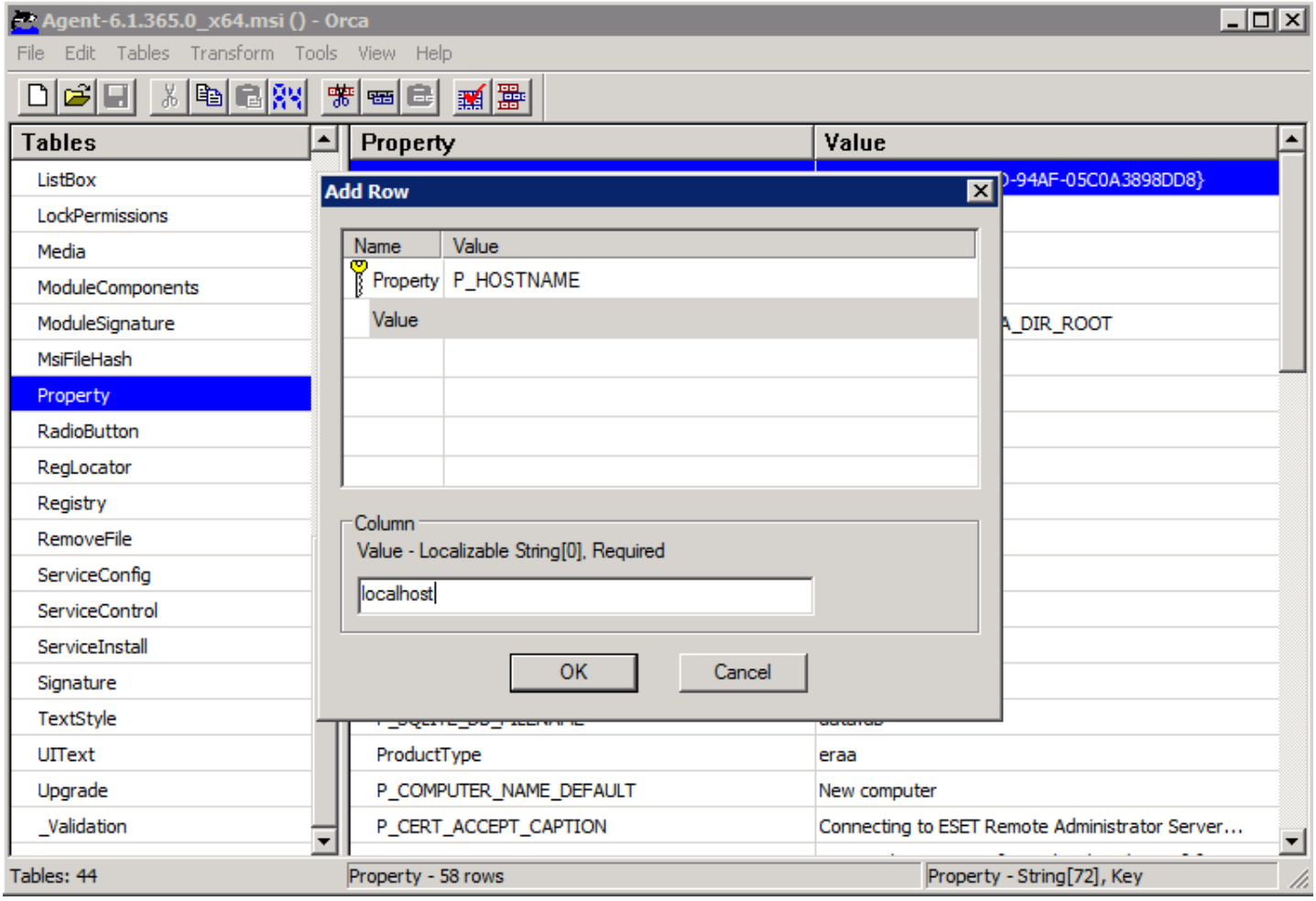
1. Install Orca (it is part of the Windows SDK). For more information about Orca see http://support.microsoft.com/kb/255905/
2. Download the **ERA Agent** installer. For example, you can use `Agent-6.1.365.0_x64.msi` which is a component of ERA version 6.1.28.0 for 64-bit systems. See our knowledgebase article for the list of ERA component versions.
3. Open Orca by clicking **Start** > **Programs** > **Orca**.
4. Click **File** in the top menu and then click **Open** and browse for `Agent-6.1.365.0_x64.msi` file.
5. Click **Transform** in the top menu and select **New Transform**.



6. Click **Property**.



7. Right-click anywhere in the list of property values and select **Add Row** from the context menu.
8. Add the property **P_HOSTNAME** and type the hostname or IP address of your ERA Server into the **Value** field.
9. Repeat steps 7 and 8 to add the property **P_PORT**, where the value is the port used to connect to your ERA Server (2222) by default.

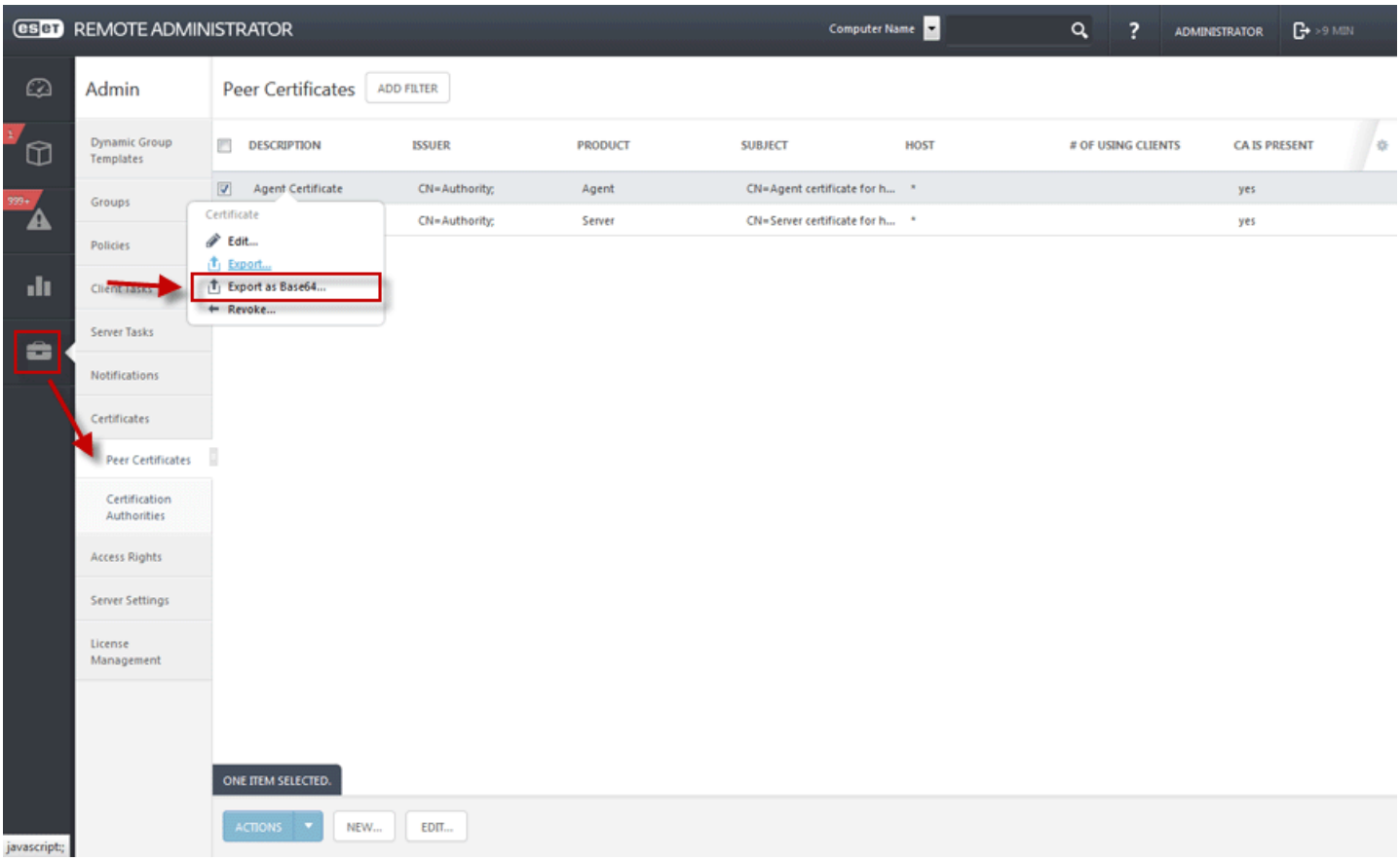


10. For ERA Agent, insert the Peer certificate (.pfx) signed by your Certificate Authority stored in ERA Server's database. Insert the Public key of the Certificate Authority (`.der` file) which was used to sign your ERA Server Peer certificate.

- **There are two ways to insert certificates:**

1. You can insert the contents of the certificate and public key encoded in **Base64 format** (no certificate files will be needed).

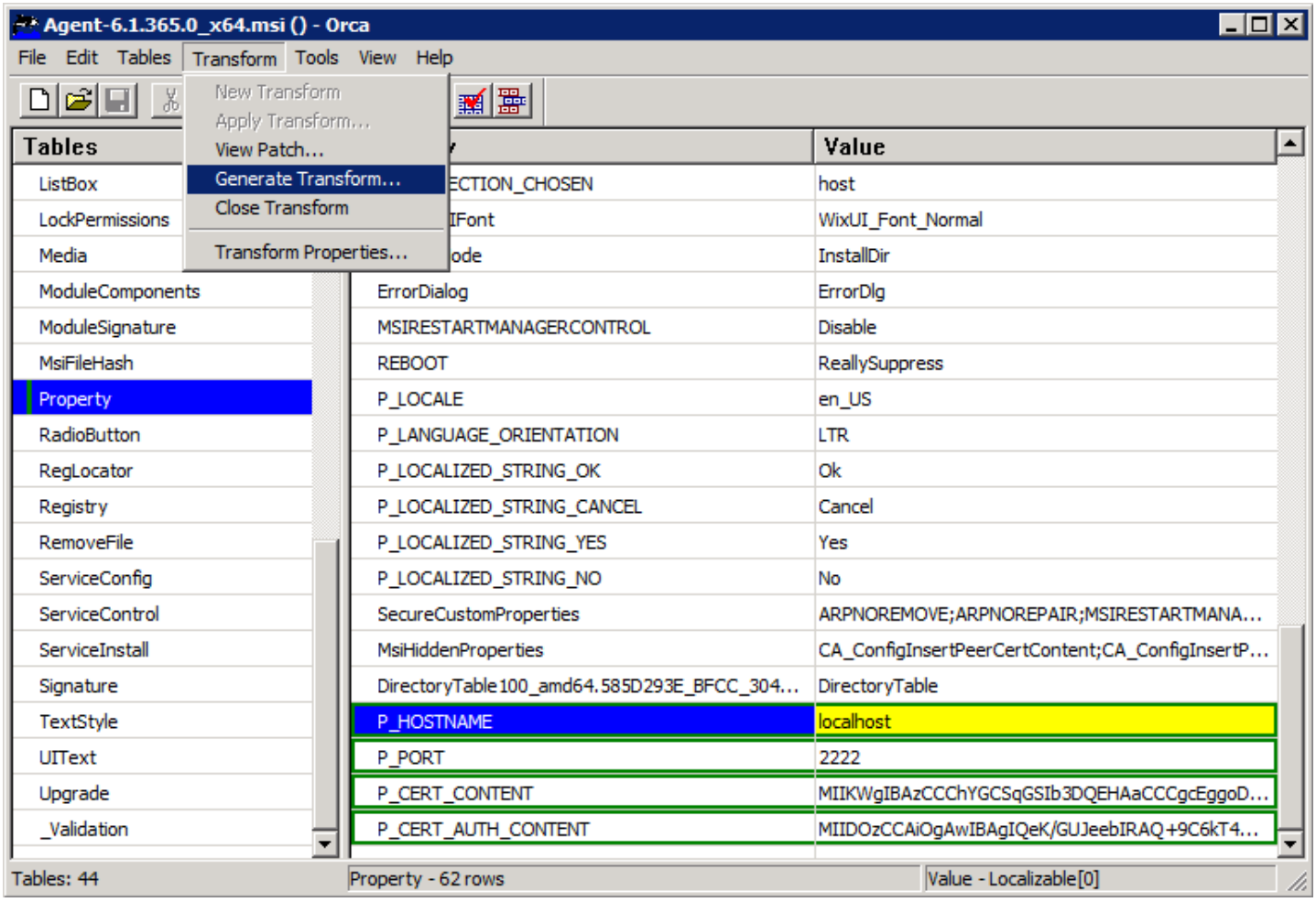
- In ERA Web Console, navigate to to **Admin** > **Certificates** > **Peer Certificate**, click Agent Certificate and choose **Export as Base64...**.
- Navigate to **Admin** > **Certificates** > **Certification Authorities**, click ERA Certificate Authority and choose **Export Public Key as Base64**



- Add the contents of the exported certificate and public key into the Property table in Orca using the following property names:

Property name	Value
P_CERT_CONTENT	<peer certificate in Base64 format>
P_CERT_PASSWORD	<password for the peer certificate (don't add this when password is empty)>
P_CERT_AUTH_CONTENT	<exported public key of the Certificate Authority in Base64 format>

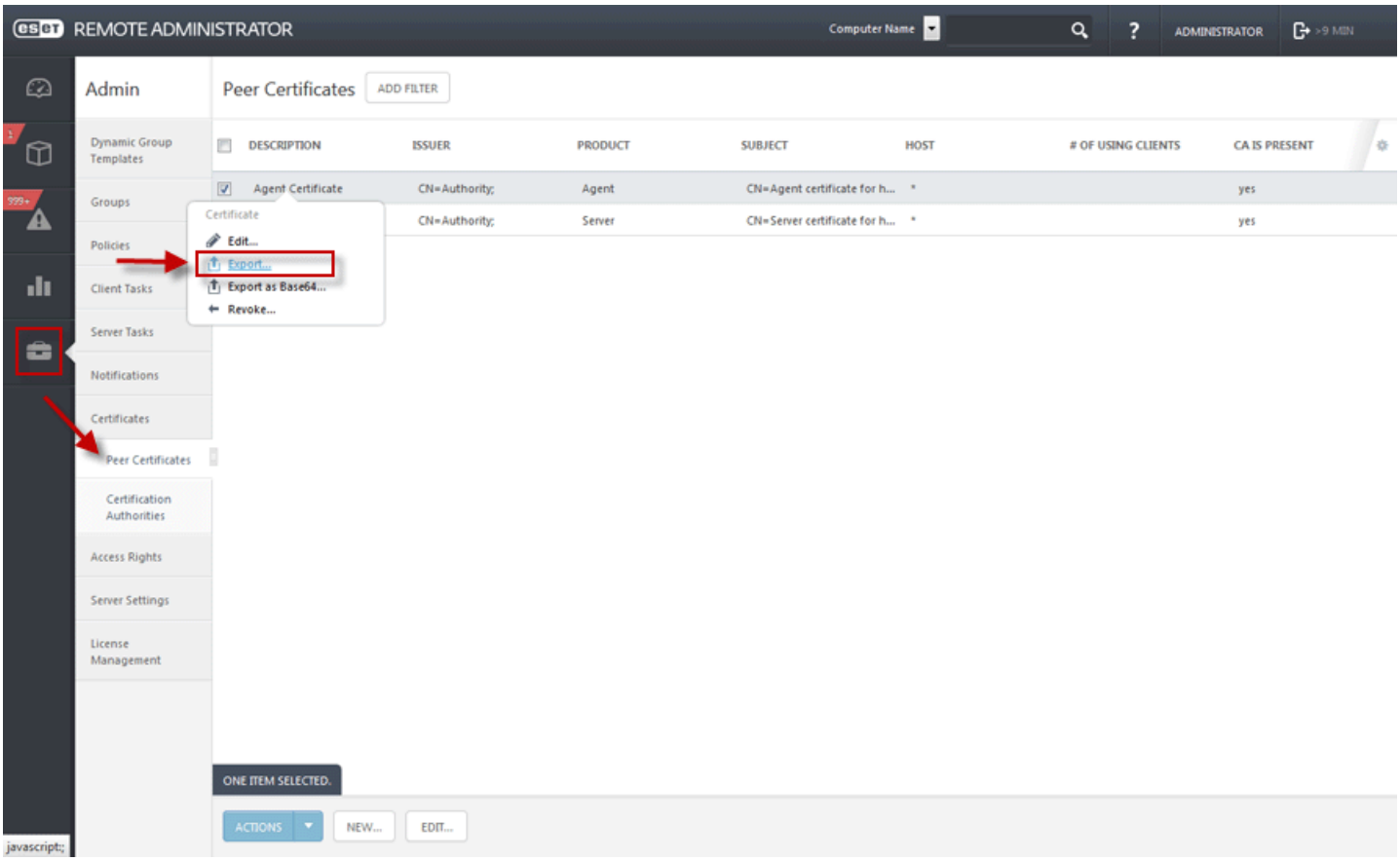
- New properties will be highlighted in green, click **Transform** and select **Generate transform...** to create a `.mst` file.



2. You can download the certificate files and make them accessible from the target machine. Export the **Agent Peer Certificate** and **Public Key** file from **Certificate Authority** of ERA Server and place them into a folder accessible from the target machine where ERA Agent will be installed.

NOTE: This option is **recommended** in specific cases.

- Go to **Admin** > **Certificates** > **Peer Certificate**, click **Agent Certificate** and choose **Export...**
- Go to **Admin** > **Certificates** > **Certification Authorities**, click **ERA Certificate Authority** and choose **Export Public Key**



- Use the exported files and add their path into the Properties table with Orca using following property names:

Property name	Value
P_CERT_PATH	<path to the exported `.pfx` certificate>
P_CERT_PASSWORD	<password for the `.pfx` certificate (don't add this when password is empty)>
P_CERT_AUTH_PATH	<path to the exported Public Key of the Certificate Authority>

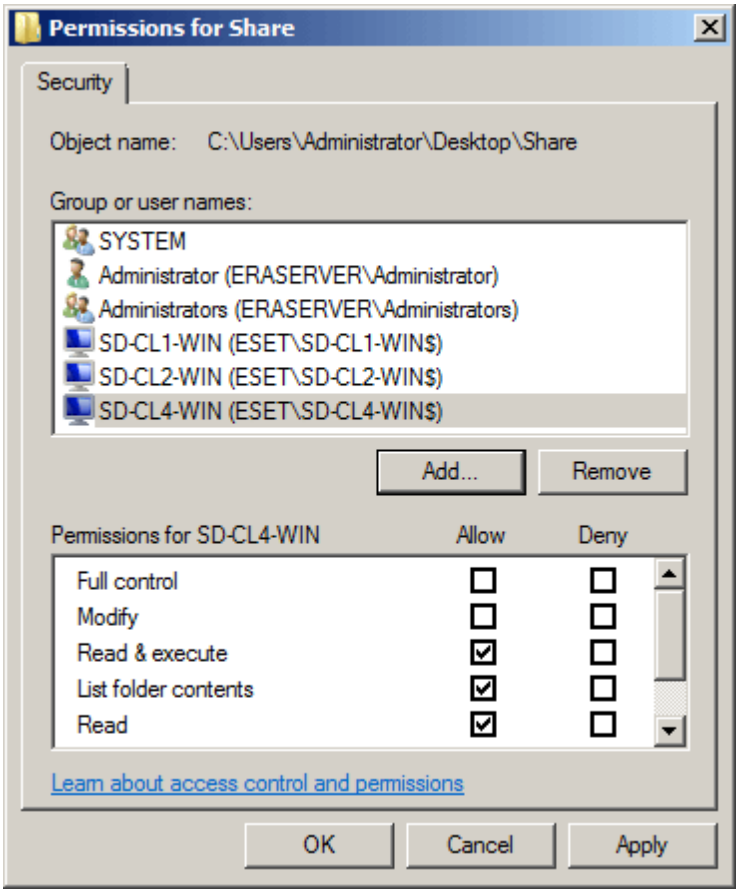
- The added properties will be highlighted in green, click **Transform** and select **Generate transform...** to create a `.mst` file.

4.4.3.2 Deployment steps - GPO

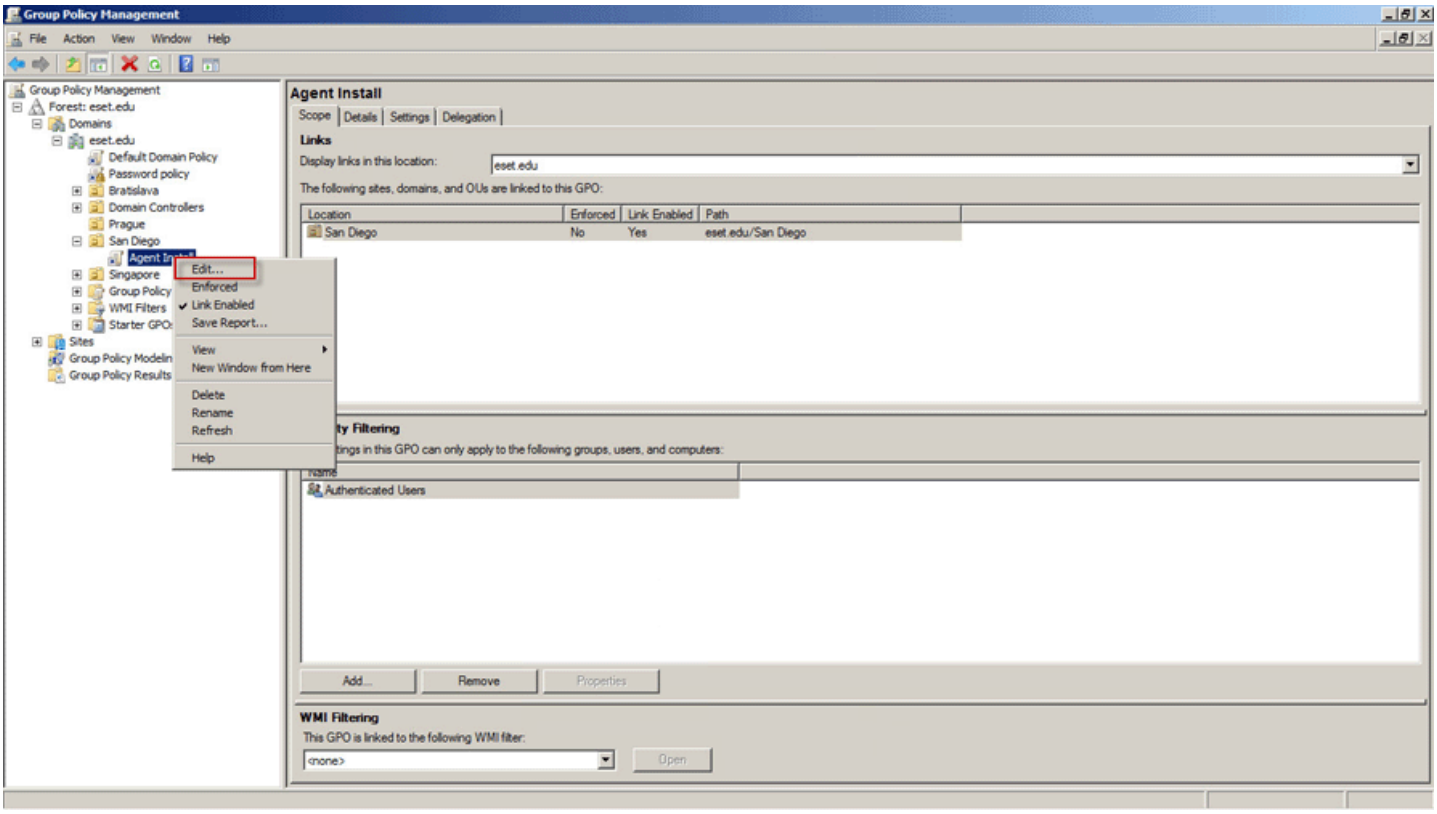
Follow the steps below or see our Knowledgebase article to deploy the ERA Agent to clients using GPO:

1. Download the ERA Agent installer `.msi` file from ESET download page.
2. Create an ERA Agent Installer transform .mst file.
3. Put the ERA Agent installer `.msi` file and transform `.mst` file in a shared folder that can be accessed by your target client(s).

NOTE: Client computers will require read/execute access to this shared folder.

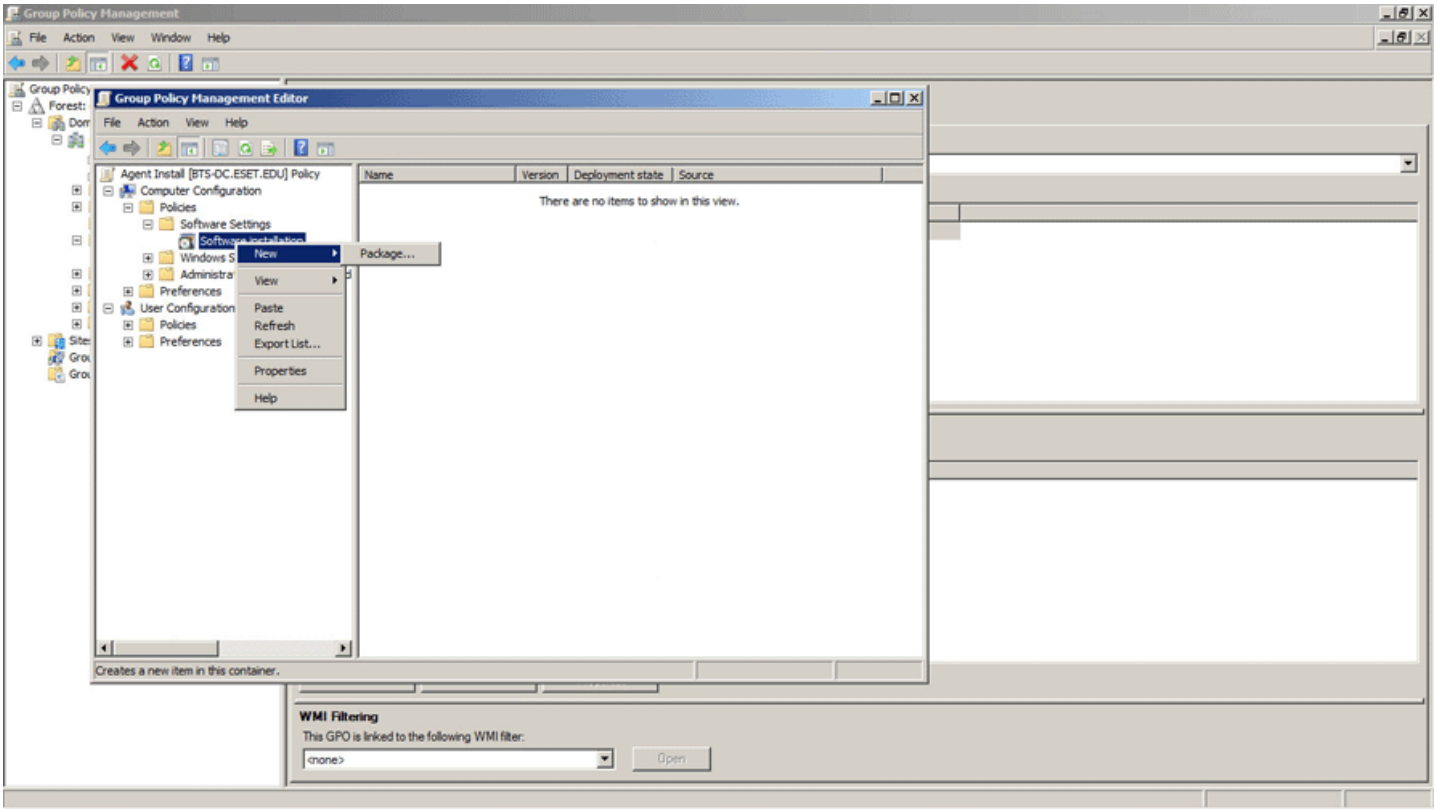


4. Use an existing Group Policy Object or create a new one (right-click GPO and click **New**). In the GPMC (Group Policy Management Console) tree, right-click the GPO you want to use and select **Edit**...



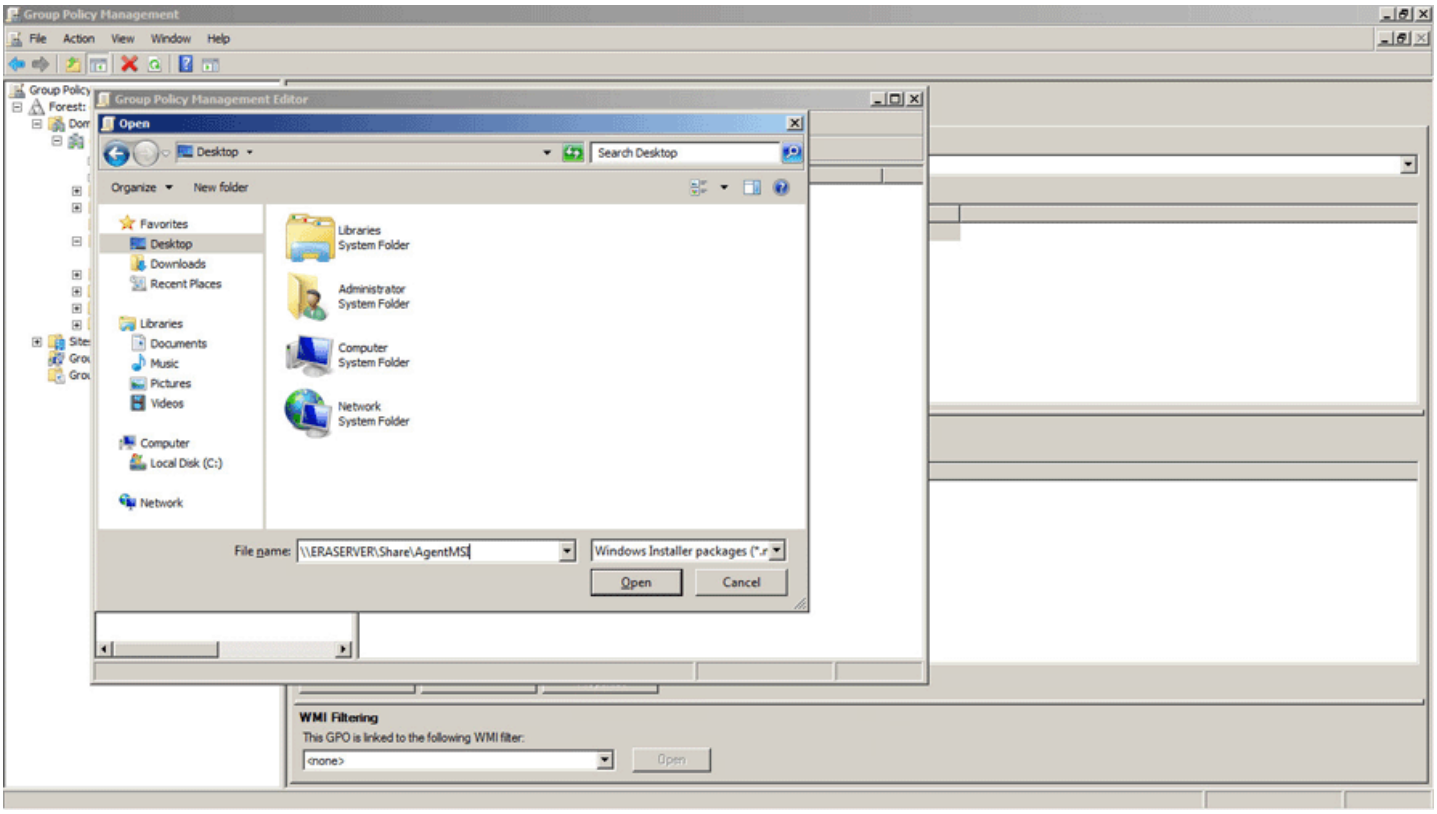
5. In Computer Configuration, navigate to **Policies** > **Software Settings** > **Software Settings**.

6. Right-click **Software installation**, select **New**, and click **Package**... to create a new package configuration.

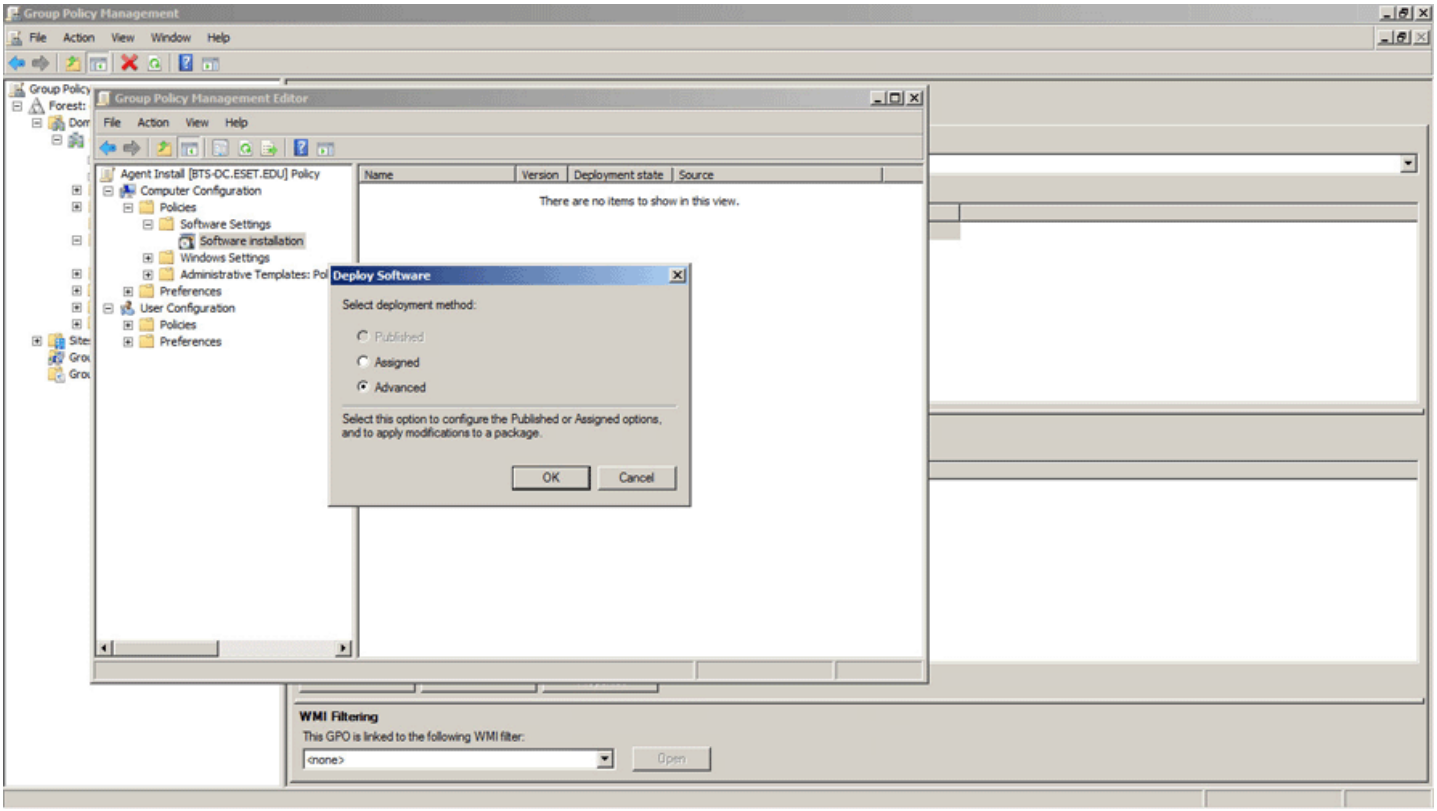


7. Browse to the location of the ERA Agent `.msi` file. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want to use. For example `\\fileserver\share\filename.msi`

NOTE: Make sure that you use the UNC path of the shared installer package.

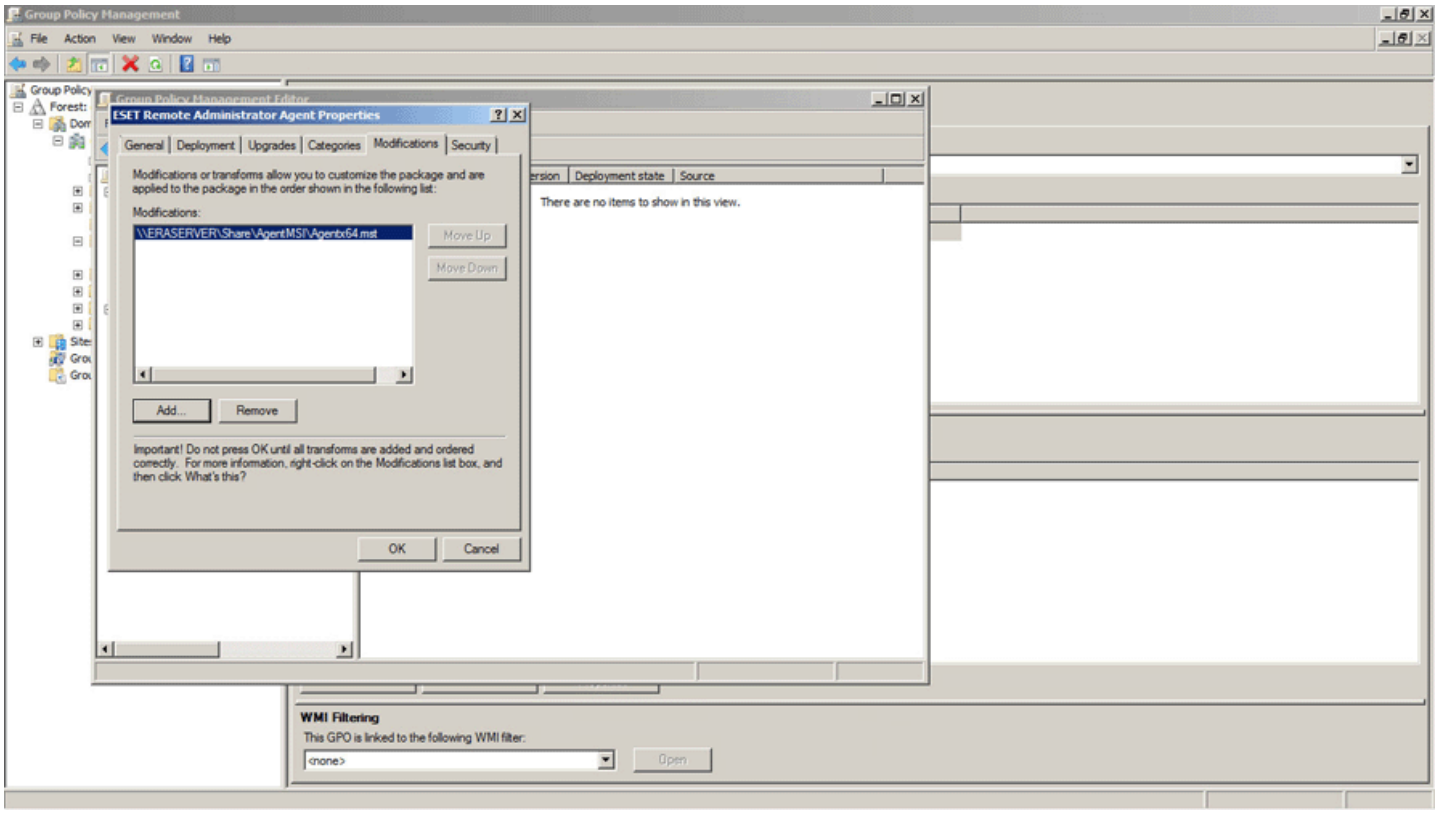


8. Click **Open** and choose the **Advanced** deployment method.

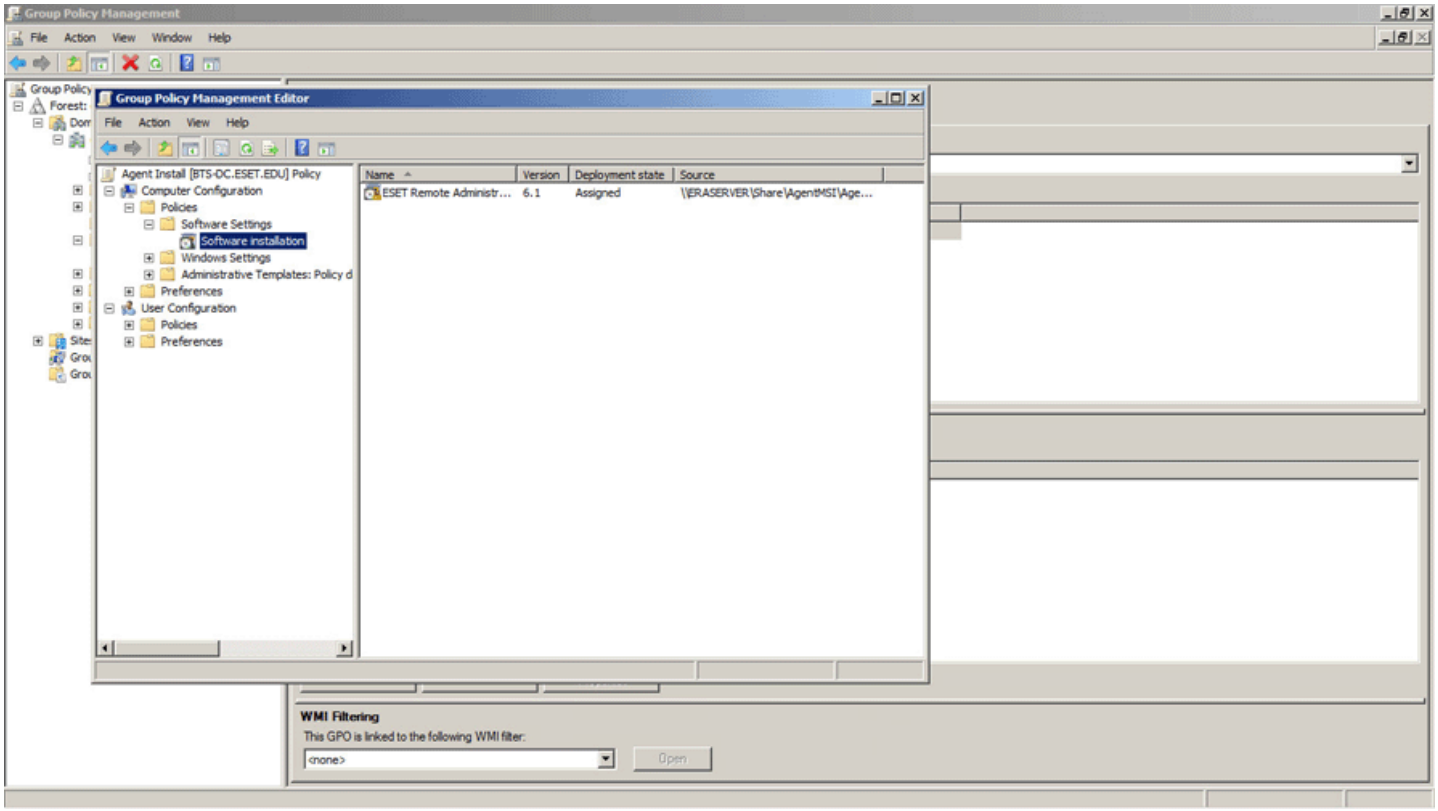


9. This will allow you to configure deployment options. Select the **Modifications** tab and browse for the ERA Agent Installer transform `.mst` file.

NOTE: The path must point to the same shared folder as the one used step 7.


Group Policy Management
File Action View Window Help
ESET Remote Administrator Agent Properties
General Deployment Upgrades Categories Modifications Security
Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:
Modifications:
\\ERASERVER\Share\AgentMSI\Agentx64.mst
Move Up
Move Down
Add...
Remove
Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?
OK
Cancel
Deployment state
Source
There are no items to show in this view.
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open

10. Confirm the package configuration and proceed with GPO deployment.

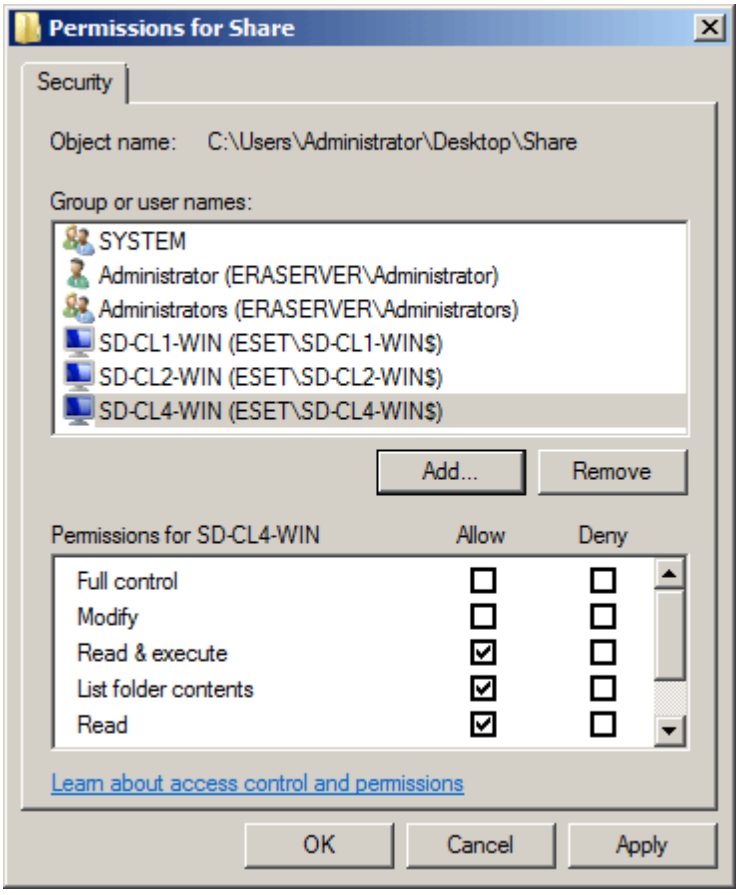


4.4.3.3 Deployment steps - SCCM

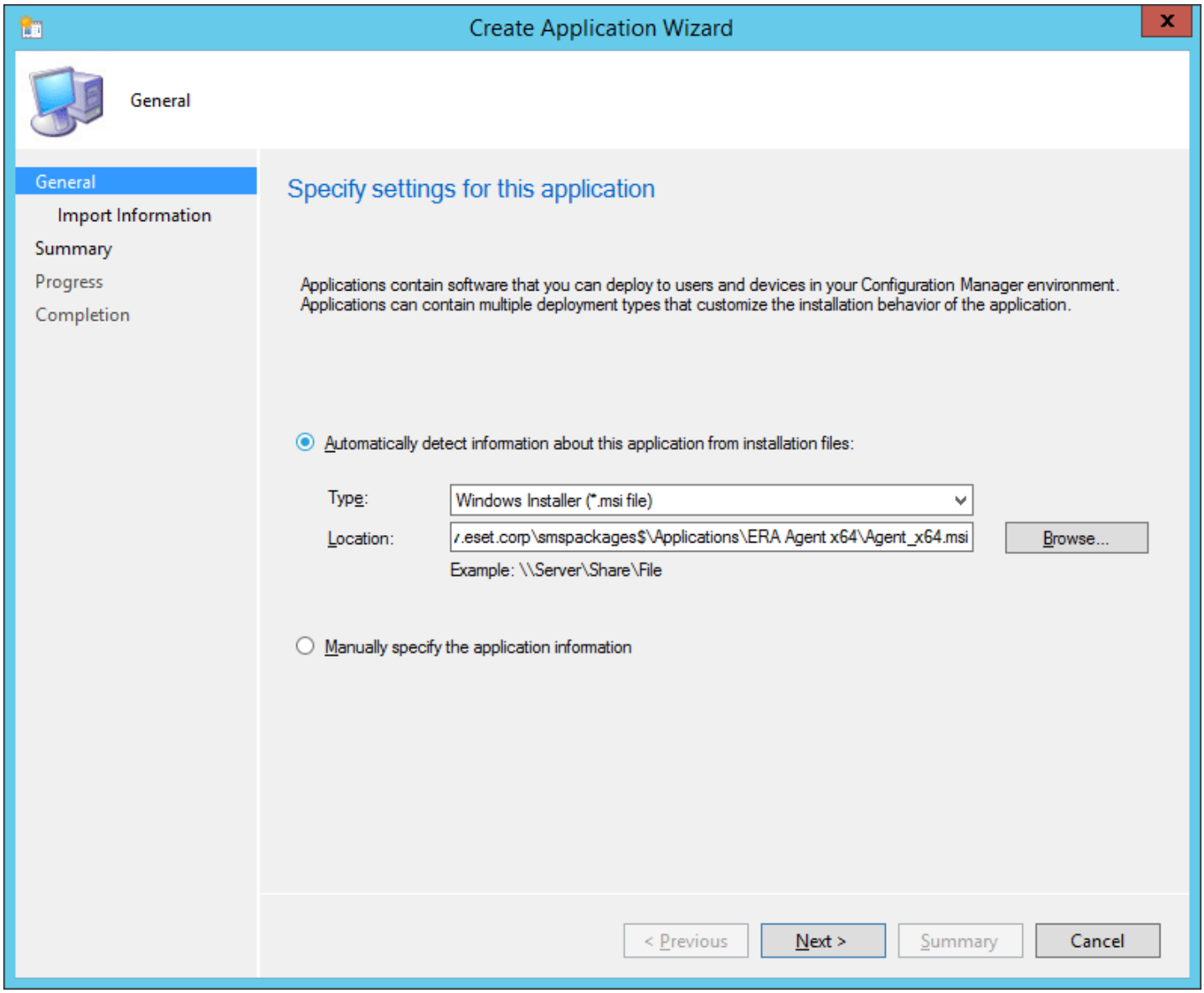
Follow the steps below or see our Knowledgebase article to deploy the ERA Agent to clients using SCCM:

1. Download the ERA Agent installer `.msi` file from ESET download page.
2. Create an ERA Agent Installer transform .mst file.
3. Put the ERA Agent installer `.msi` file and transform `.mst` file on a shared folder.

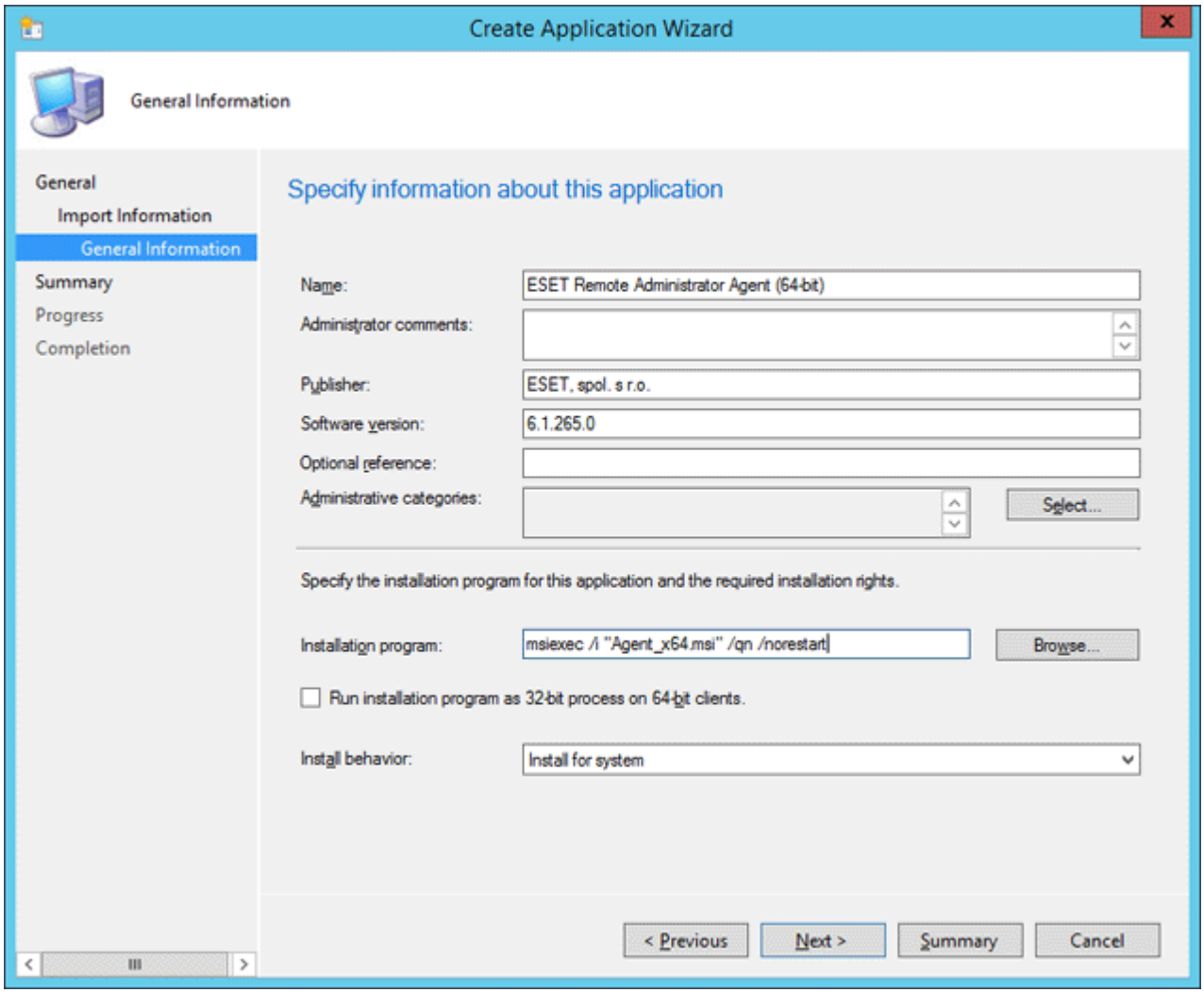
NOTE: Client computers will require read/execute access to this shared folder.



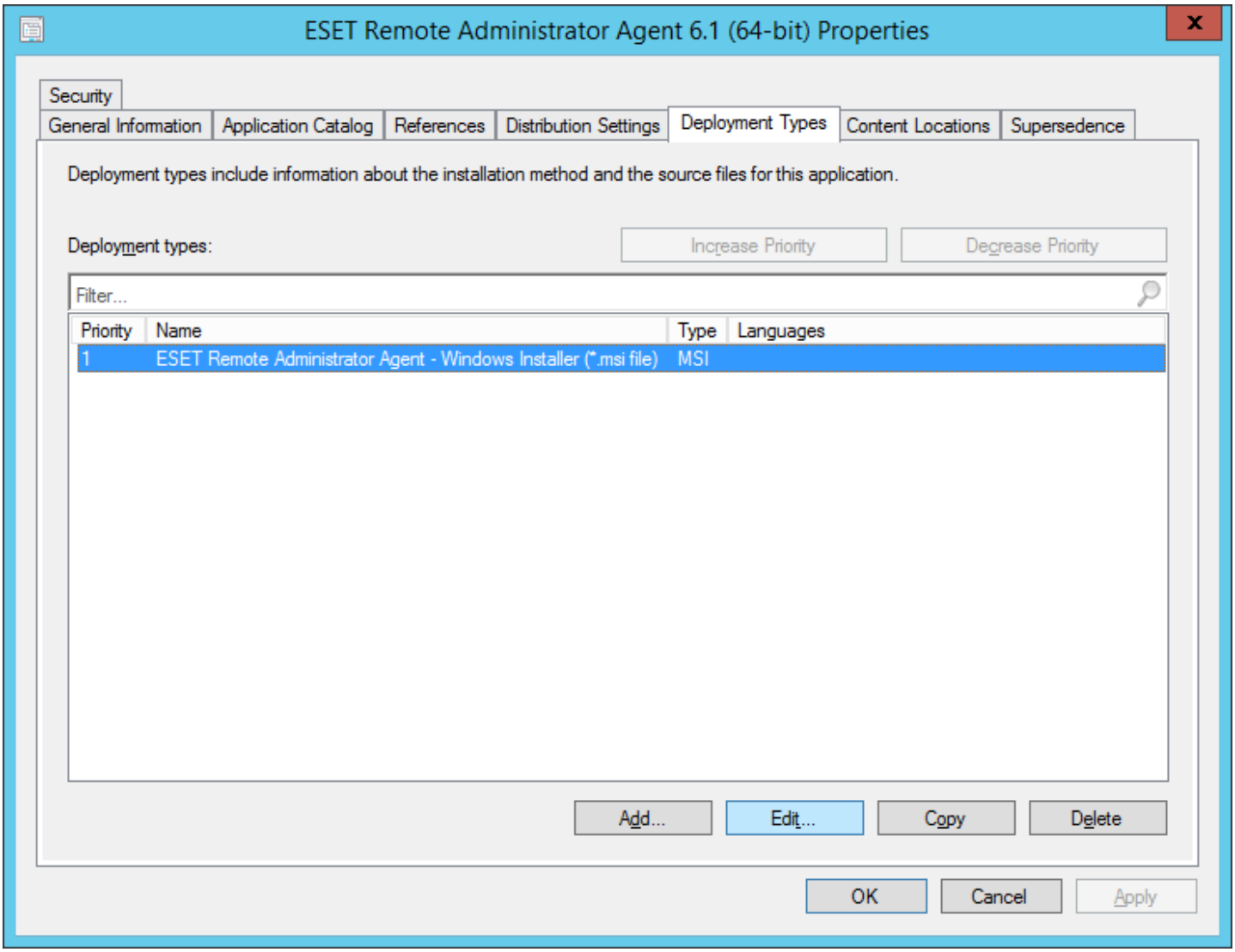
4. Open SCCM console and click **Software Library**. In **Application Management** right-click **Applications** and choose **Create Application**. Choose **Windows Installer (*.msi file)** and locate the source folder where you saved the ERA Agent installer `.msi` file.



5. Specify all required information about the application and click **Next**.

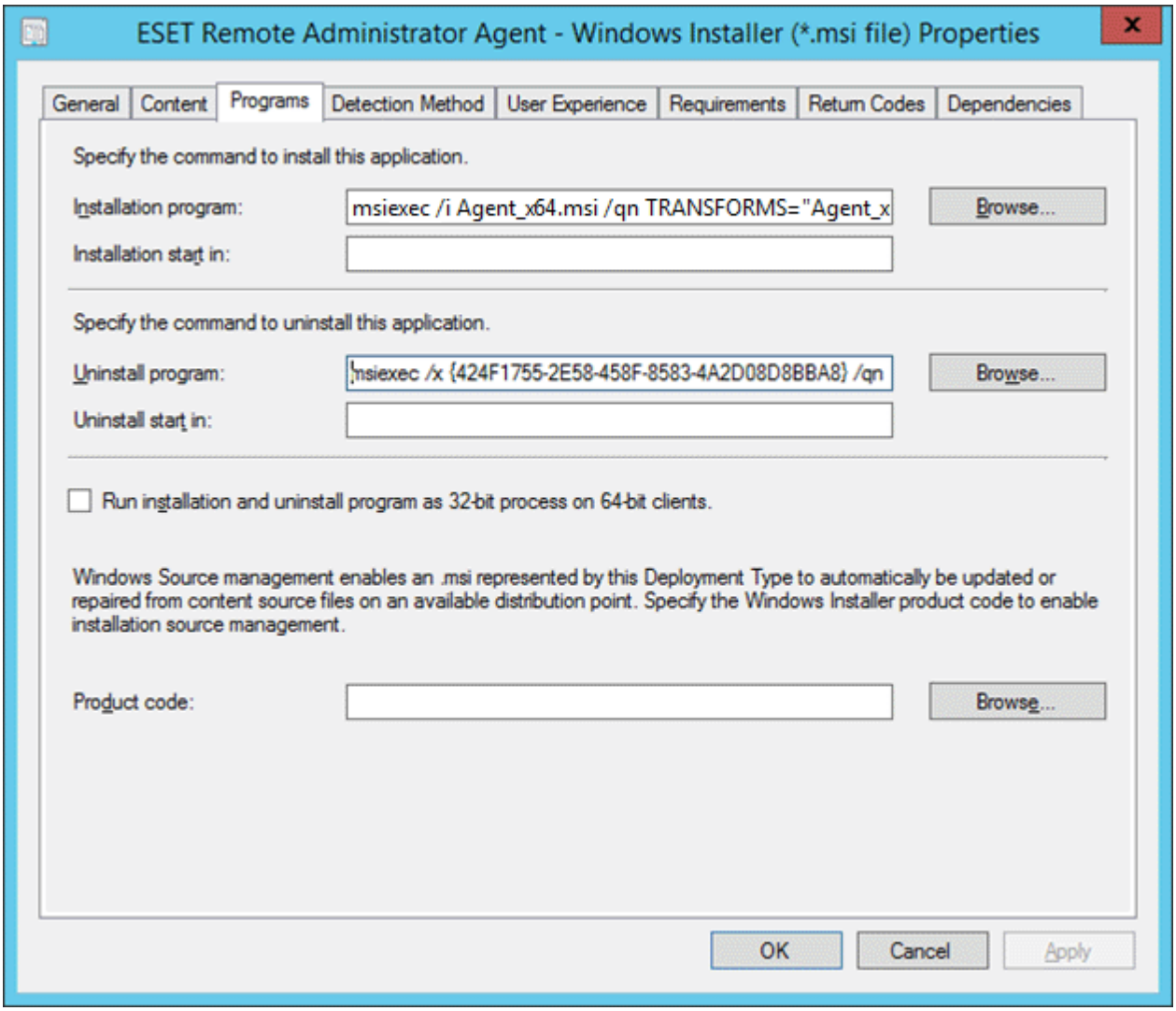


6. Right-click the ESET Remote Administrator Agent Application, click the **Deployment Types** tab, select the only deployment there and then click **Edit**.

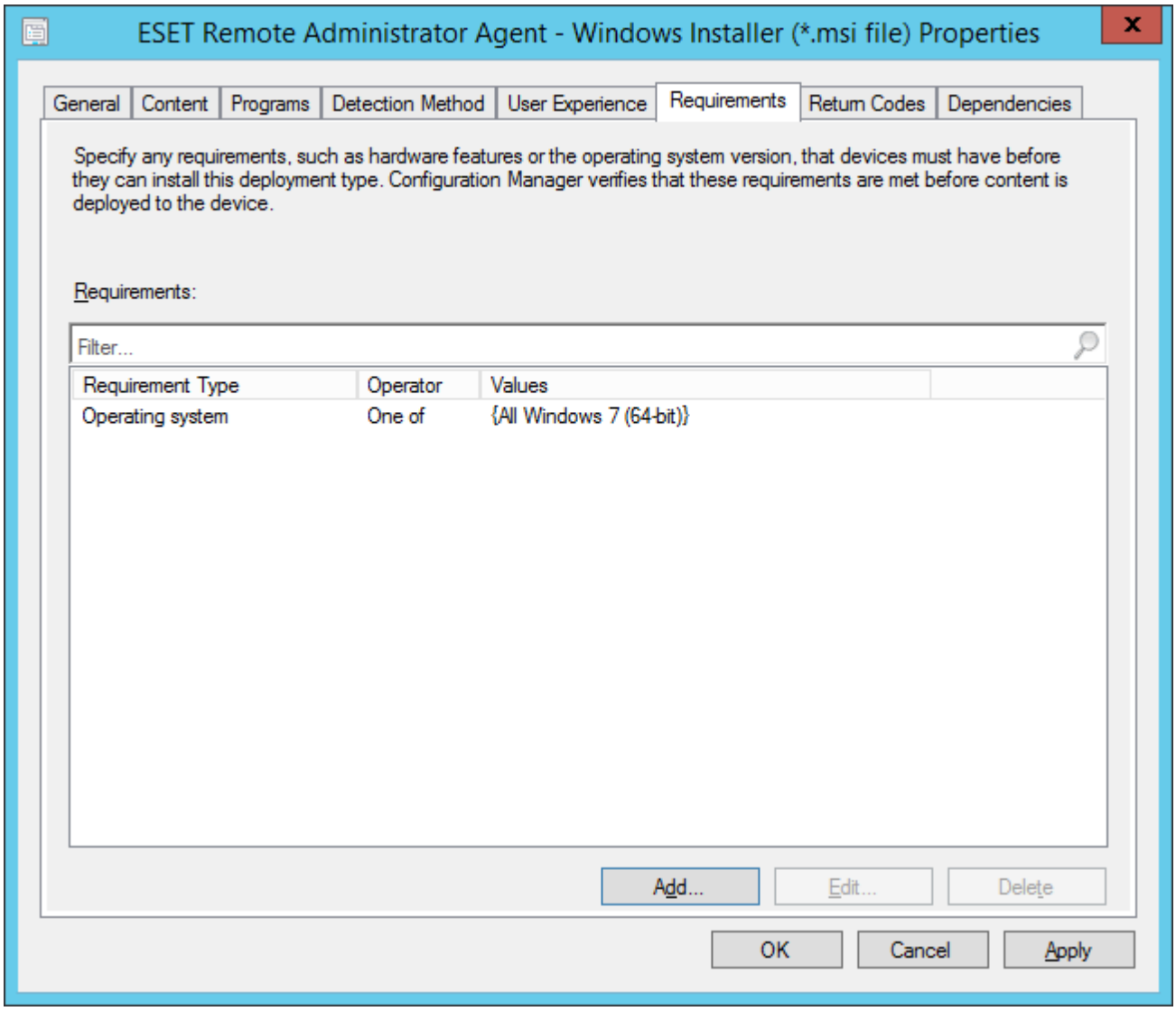


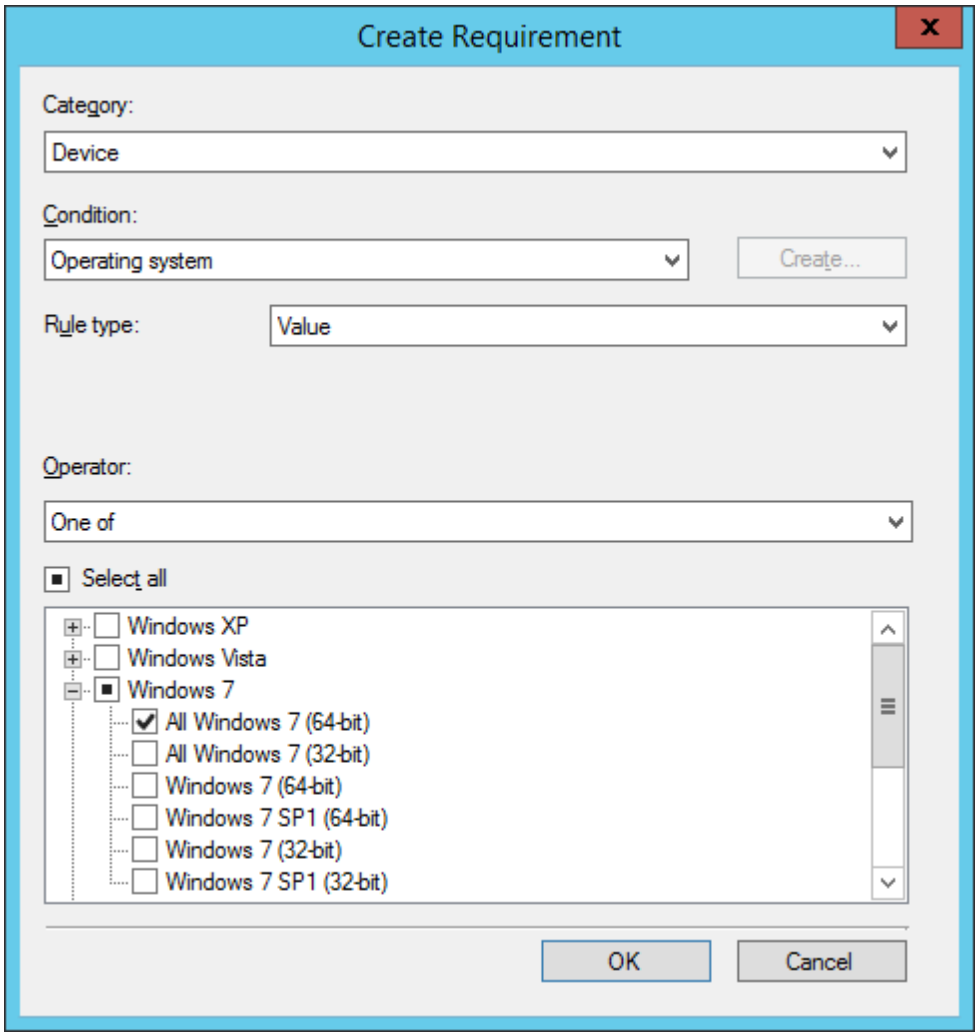
7. Click the **Porgrams** tab and edit the **Installation program** field so that it reads **msiexec/iAgent_x64.msi/qn TRANSFORMS="Agent_x64.mst** (if you are using 32-bit packages, this string will vary slightly as "x32" will appear where "x64" does in the example).

8. Edit the **Uninstall program** field so that it reads **msiexec/x {424F1755-2E58-458F-8583-4A2D08D8BBA8} /qn/ norestart**.

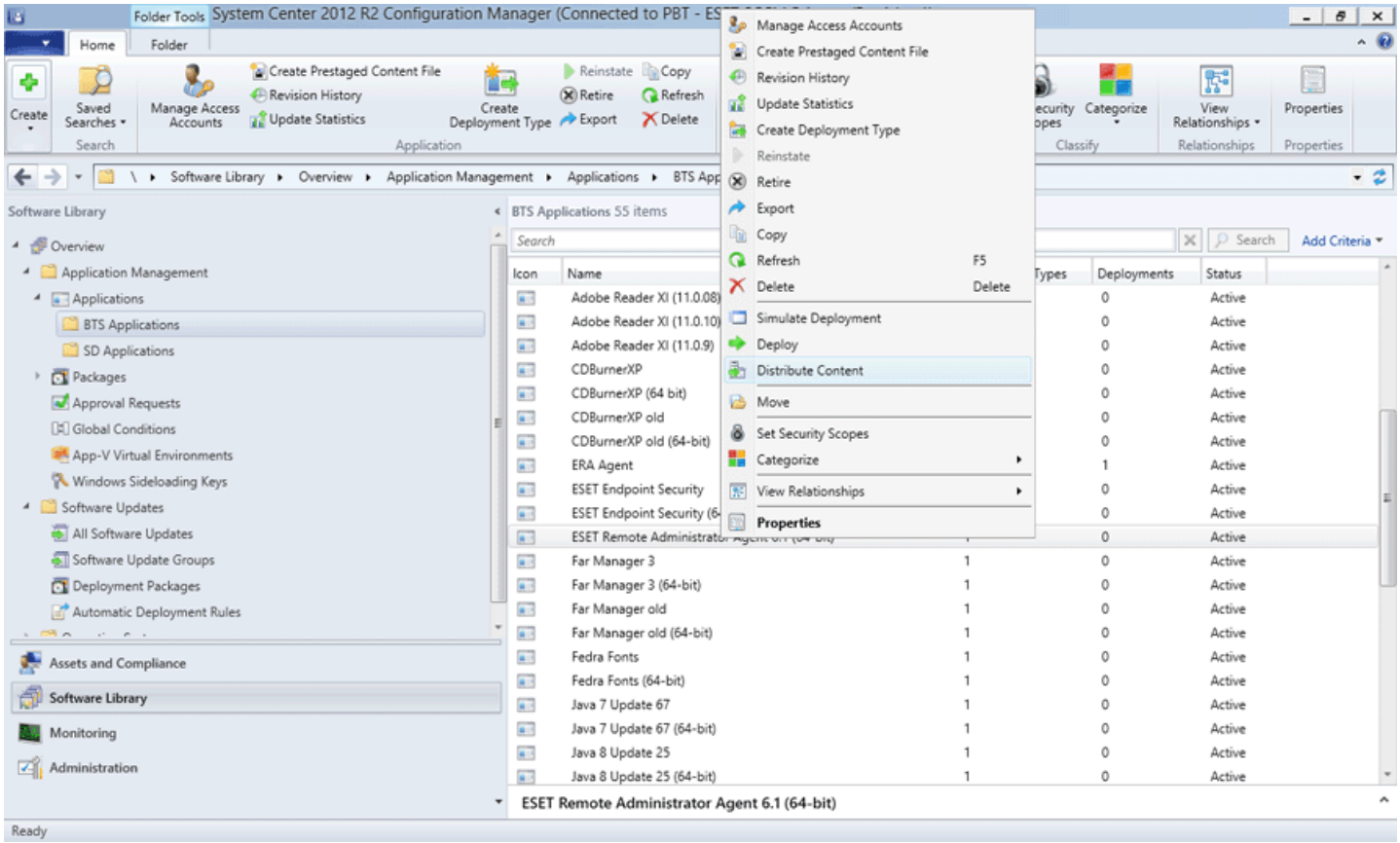

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify the command to install this application.
Installation program:
msiexec /i Agent_x64.msi /qn TRANSFORMS="Agent_x
Browse...
Installation start in:
Specify the command to uninstall this application.
Uninstall program:
msiexec /x {424F1755-2E58-458F-8583-4A2D08D8BBA8} /qn
Browse...
Uninstall start in:
Run installation and uninstall program as 32-bit process on 64-bit clients.
Windows Source management enables an .msi represented by this Deployment Type to automatically be updated or repaired from content source files on an available distribution point. Specify the Windows Installer product code to enable installation source management.
Product code:
Browse...
OK
Cancel
Apply

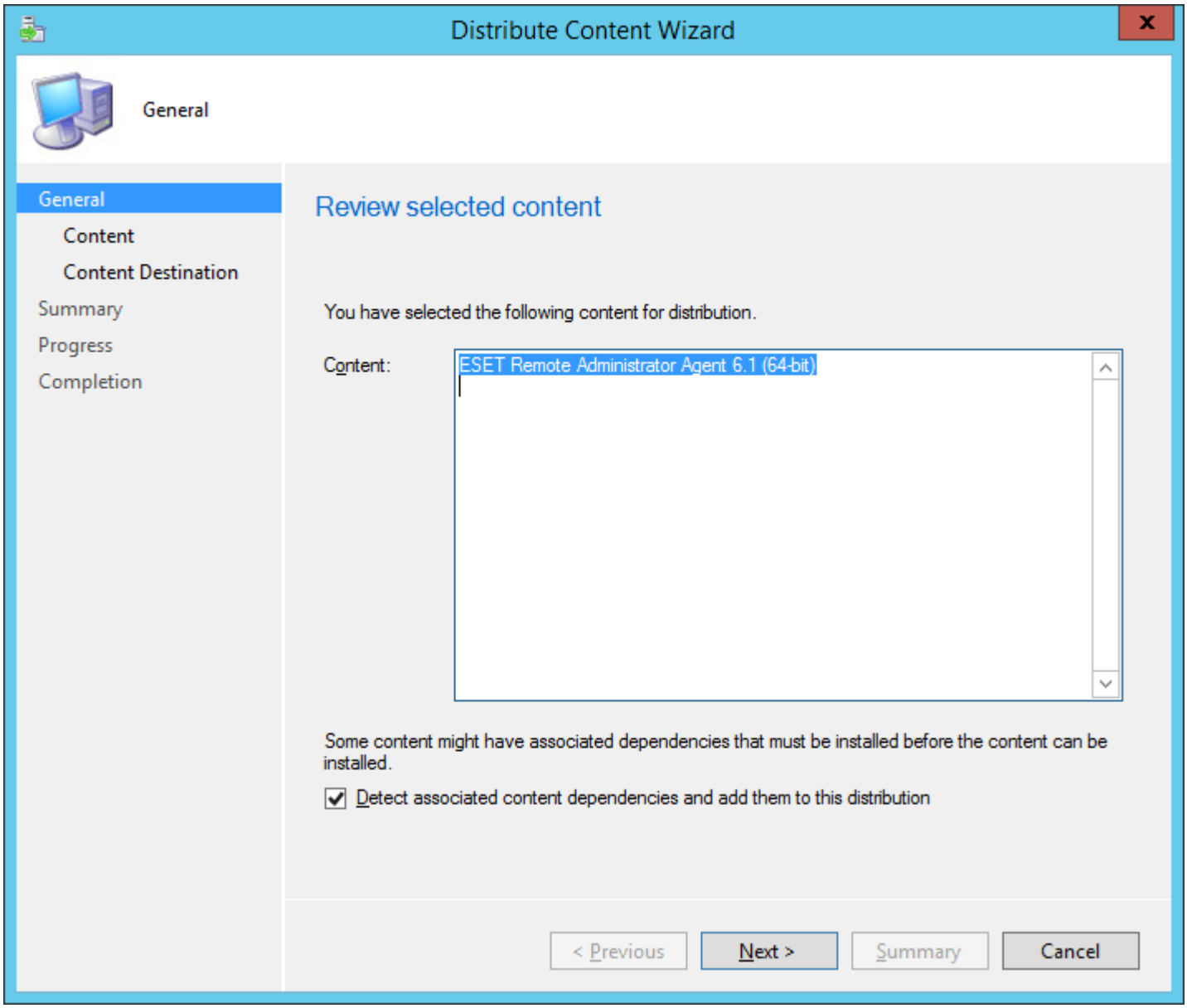
9. Click the **Requirements** tab and then click **Add**. Select **Operating system** from the **Condition** drop-down menu, select **One of** from the **Operator** drop-down menu and then specify the operating systems you will install to by selecting the appropriate check box(es). Click **OK** when you are finished and then click **OK** to close any remaining windows and save your changes.

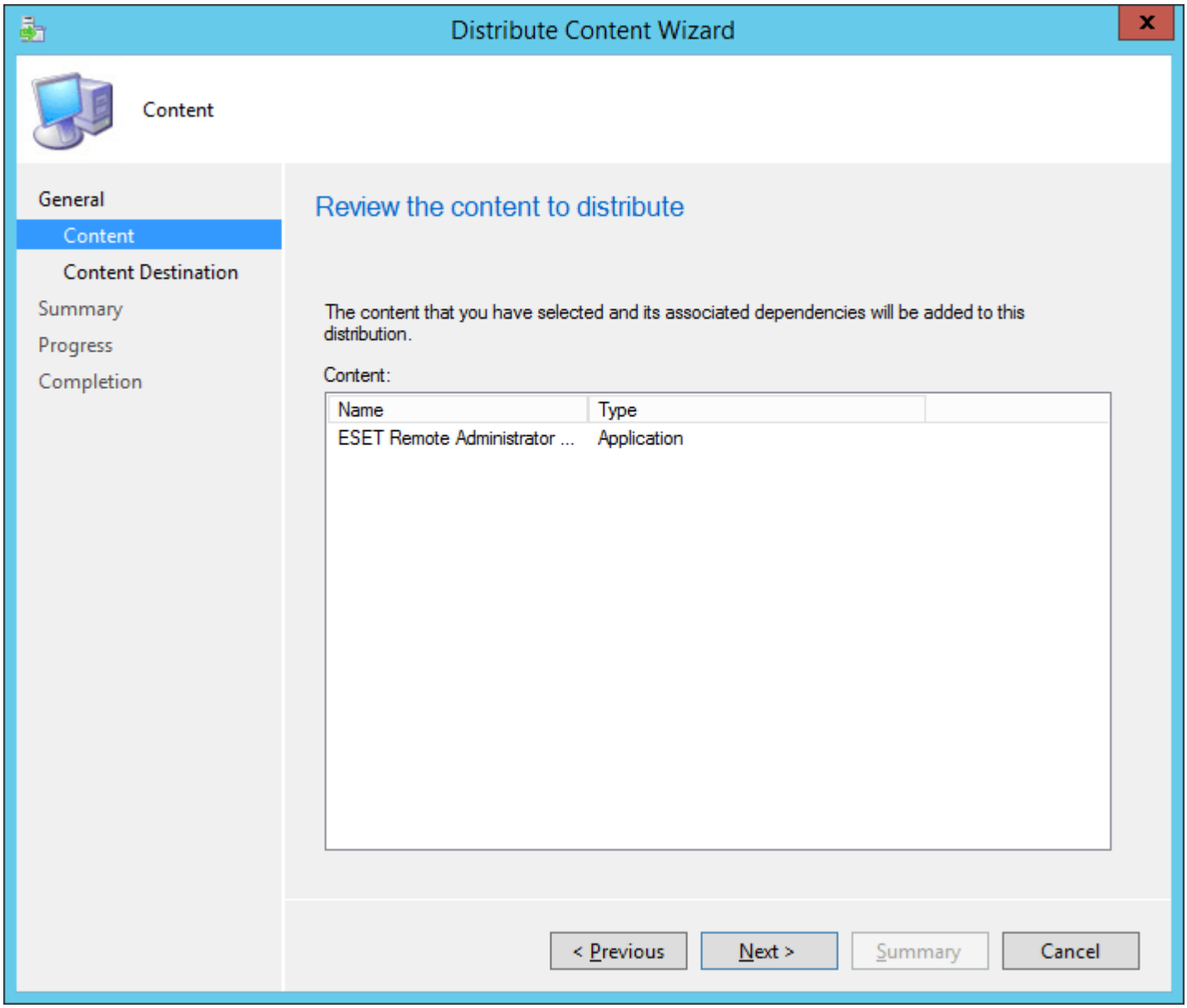

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply



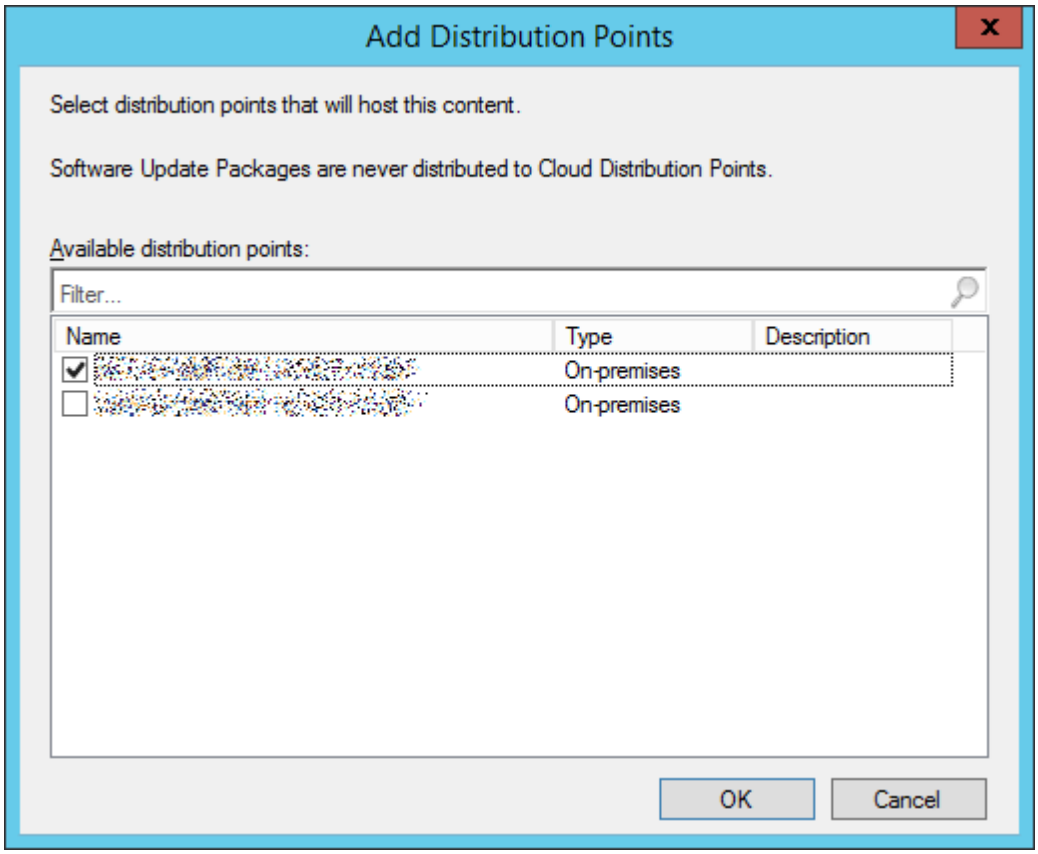
10. In the System Center Software Library, right-click your new application and select **Distribute Content** from the context menu. Follow the prompts in the Deploy Software Wizard to complete deployment of the application.

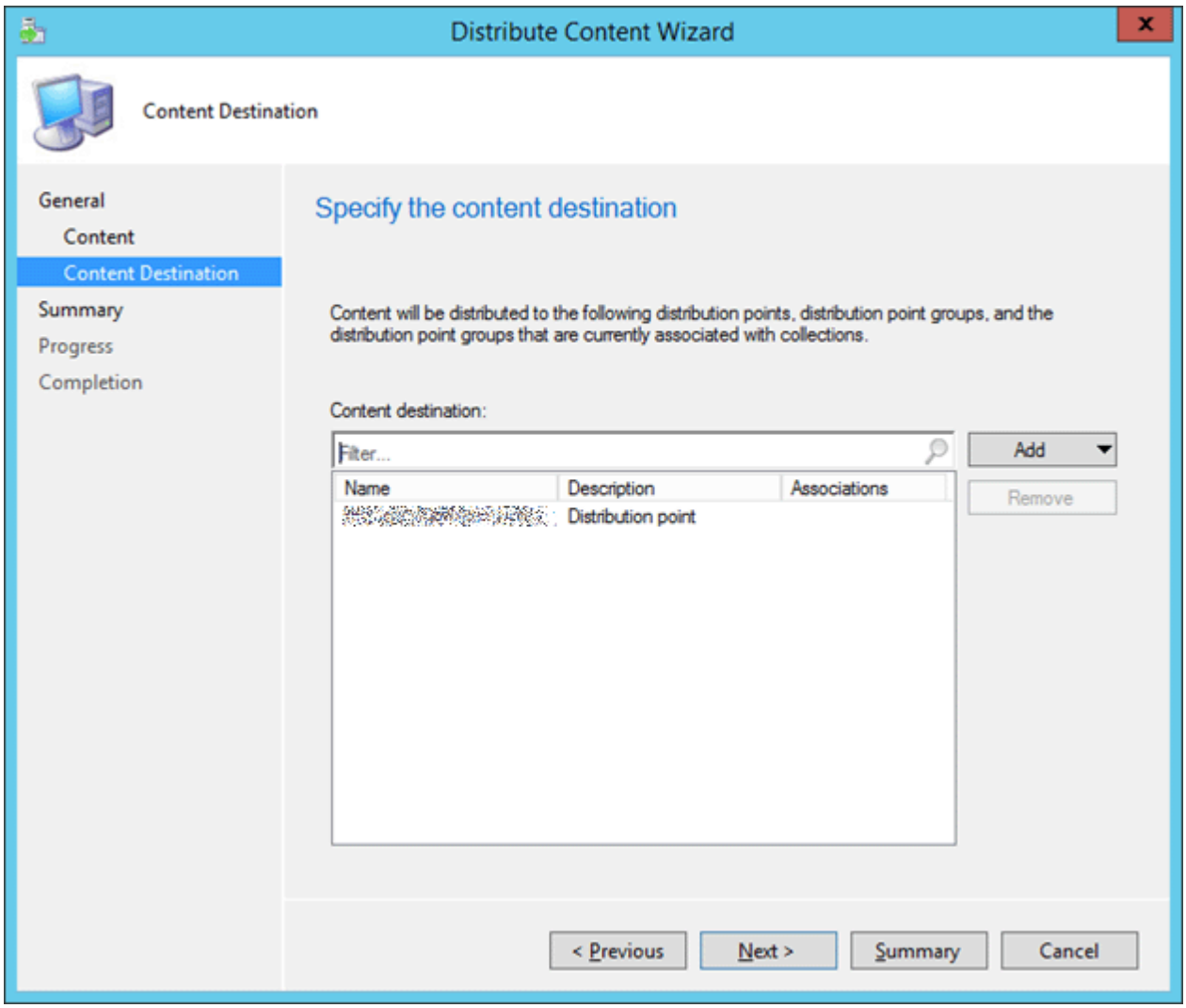


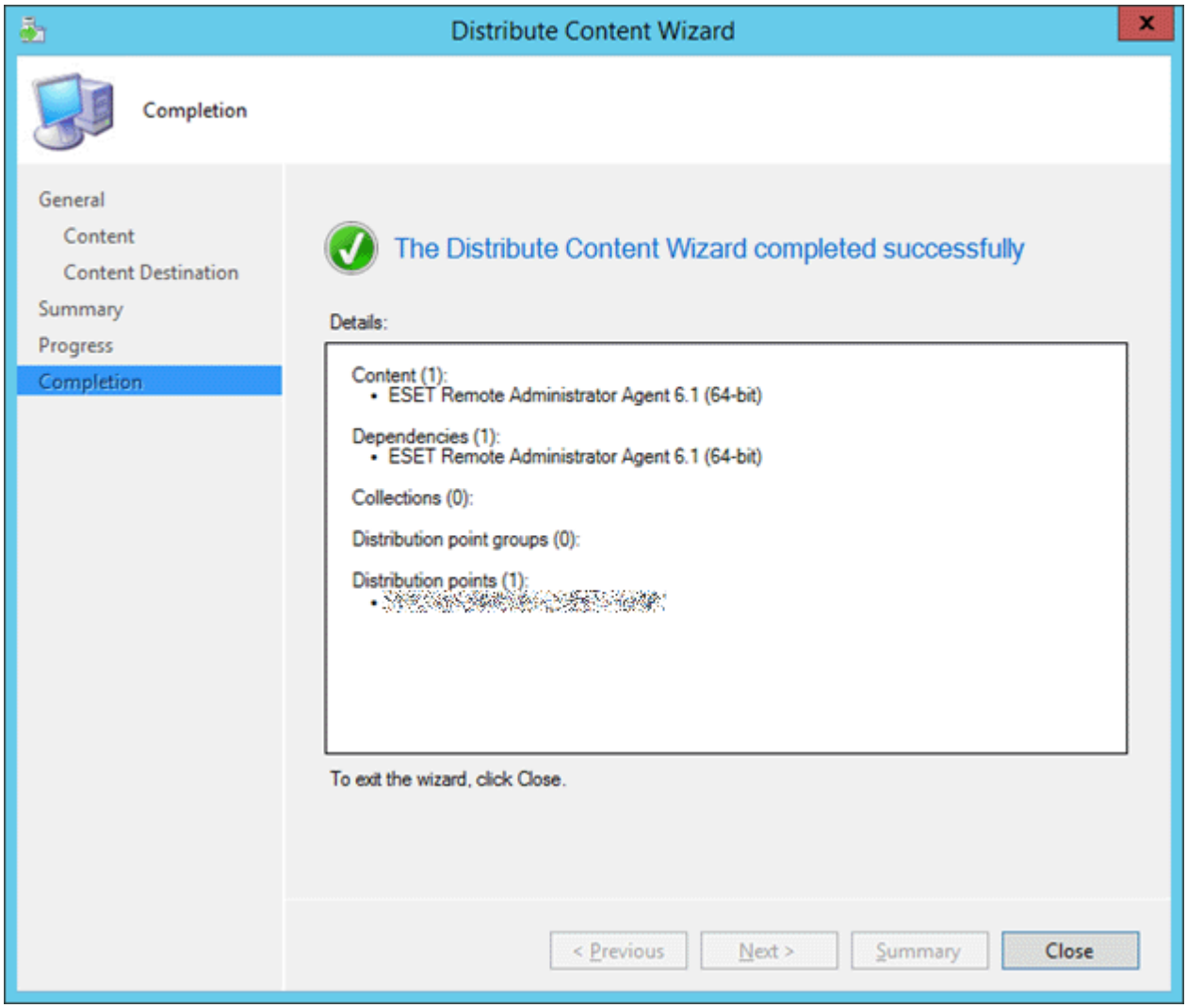

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent 6.1 (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

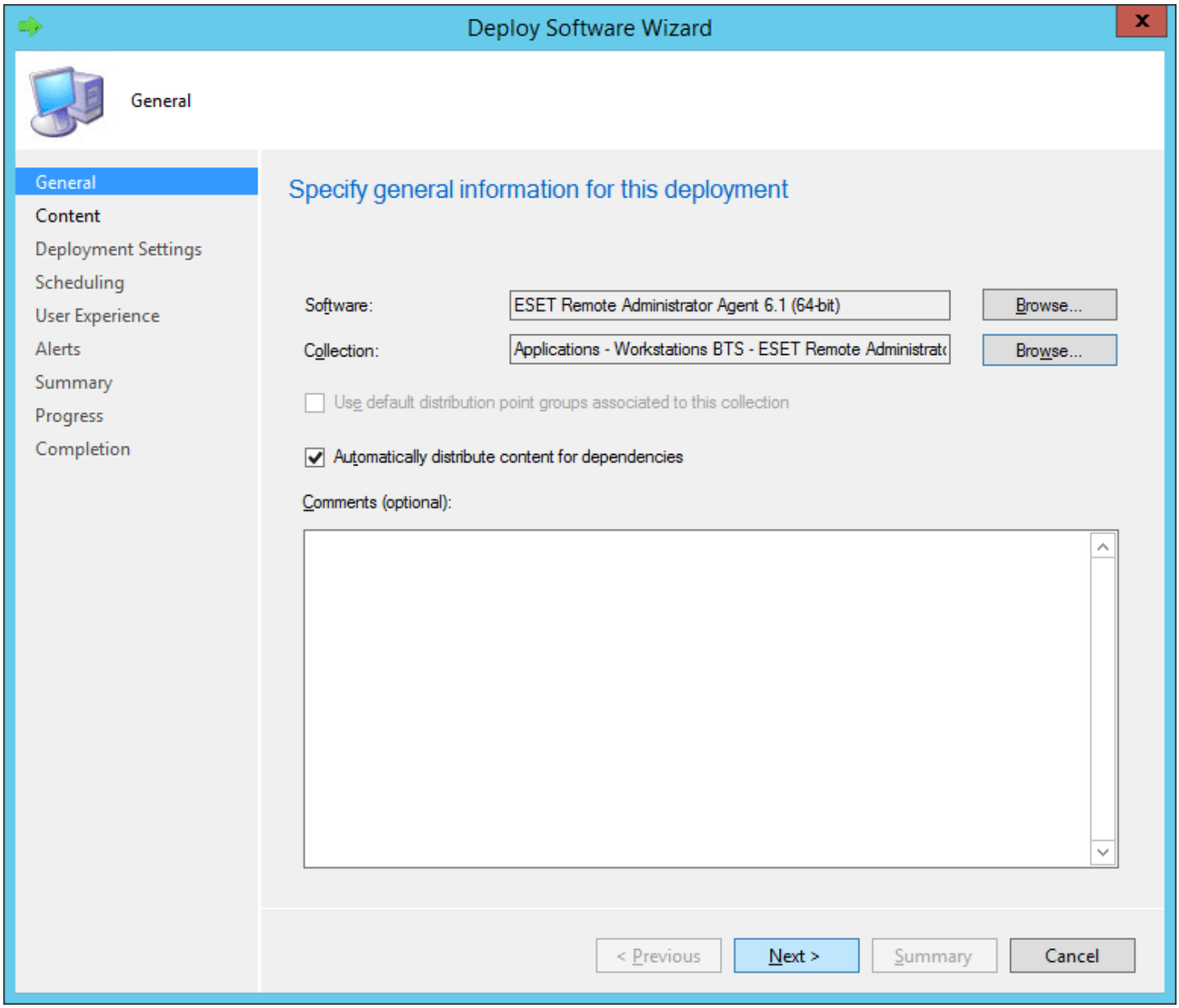


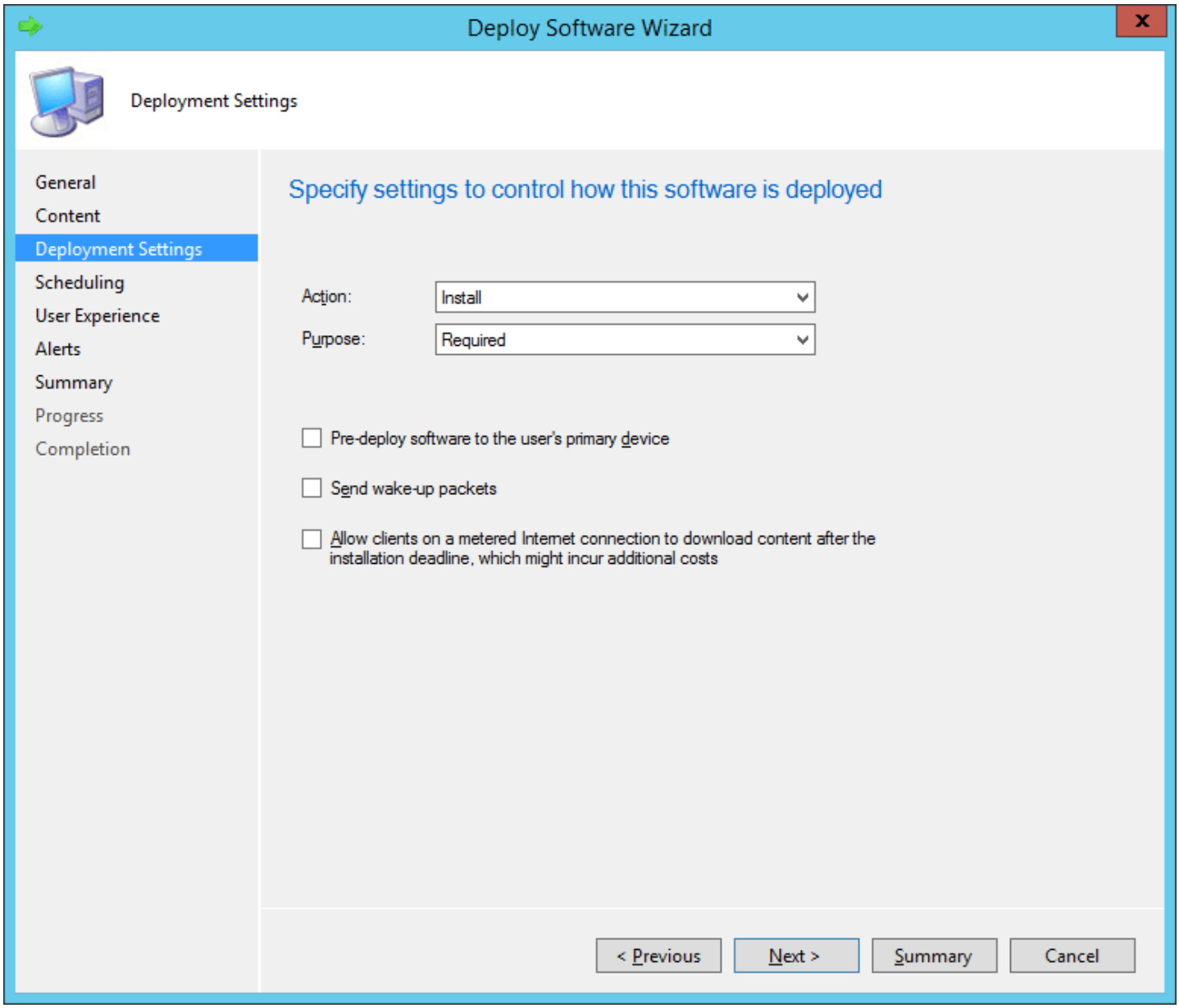
11. Right-click the application and choose **Deploy**. Follow the wizard and choose the collection and destination where you want to deploy the agent.

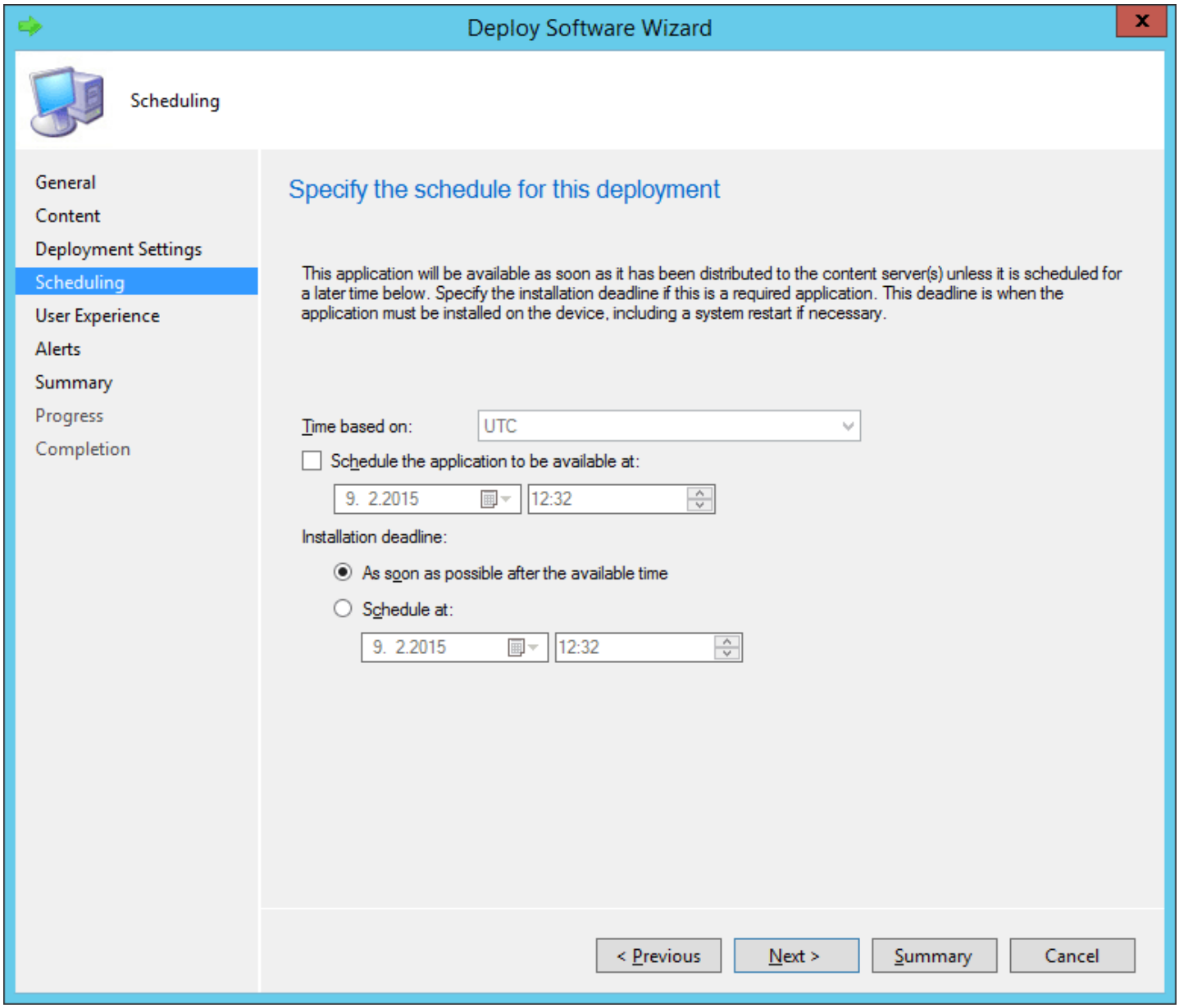

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

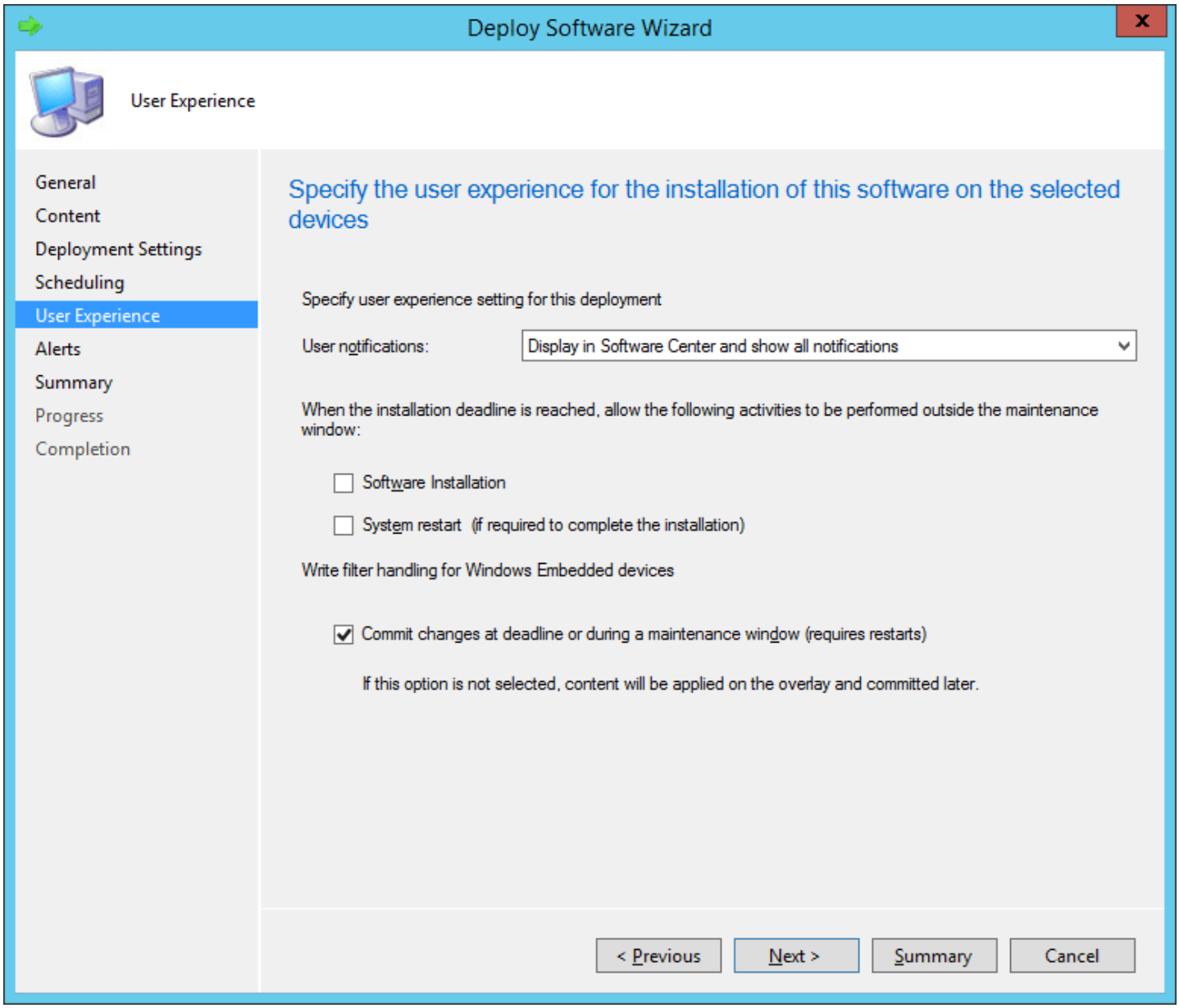

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Filter...
Add
Remove
Name
Description
Associations
Distribution point
< Previous
Next >
Summary
Cancel

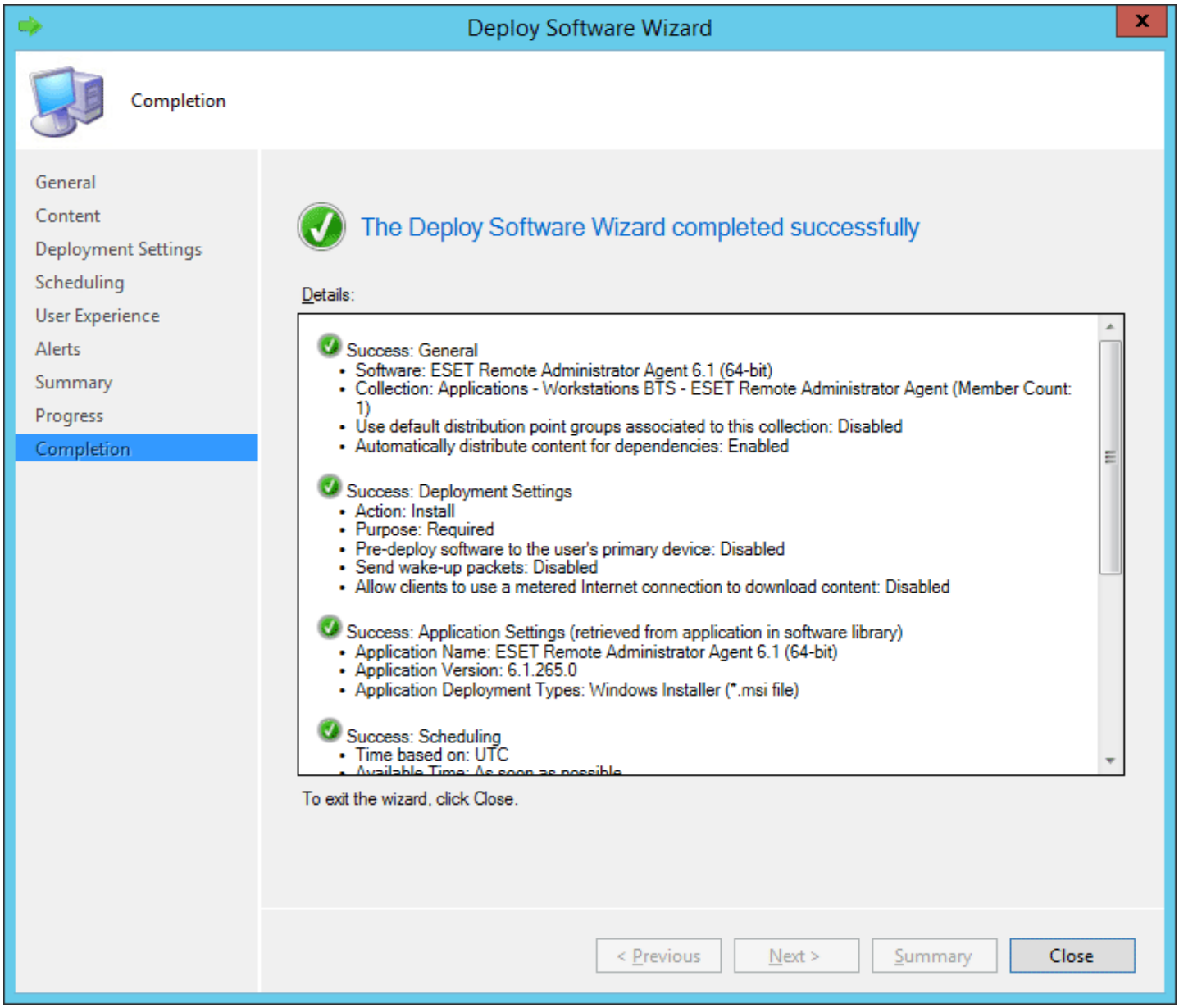

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent 6.1 (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel

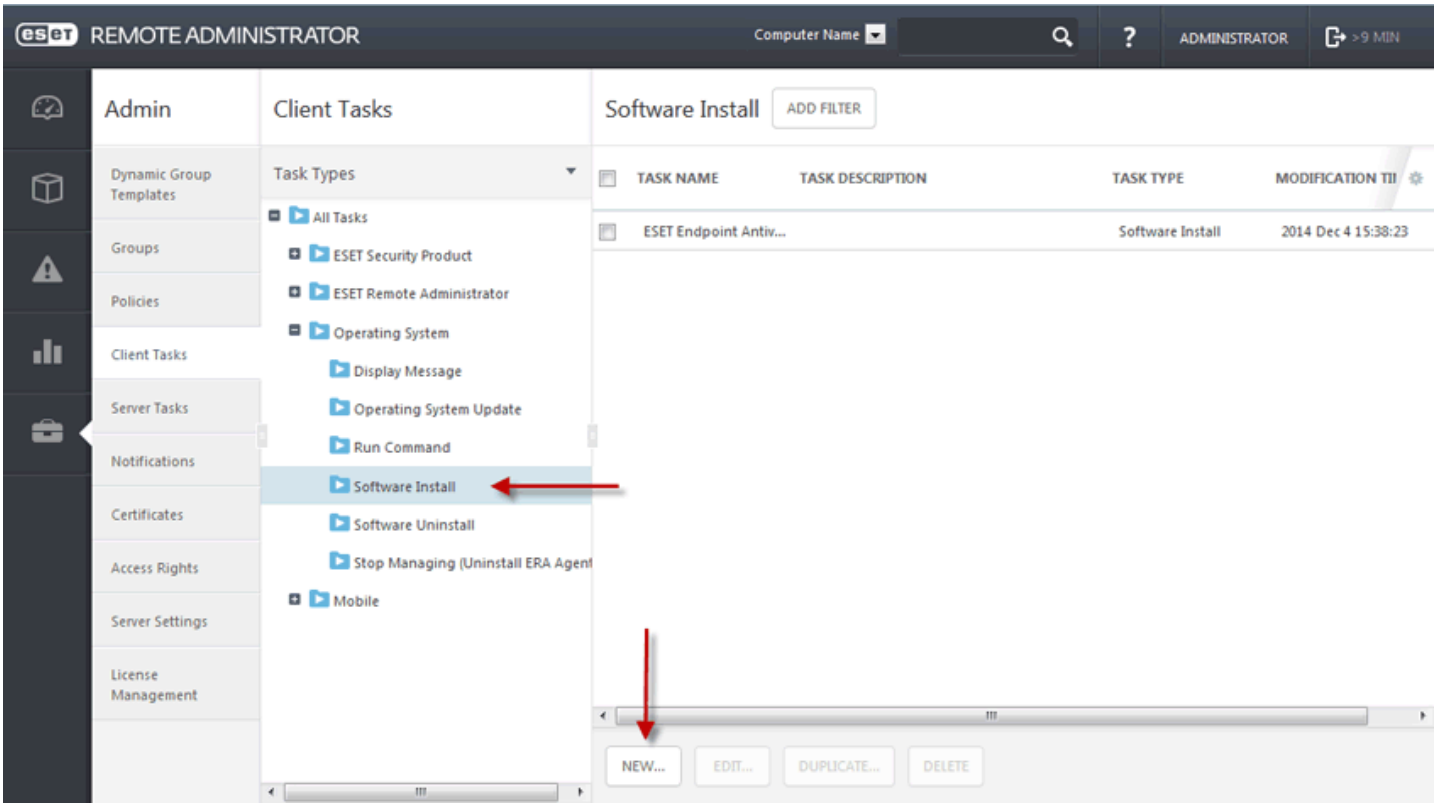

Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Completion
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
The Deploy Software Wizard completed successfully
Details:
Success: General
Software: ESET Remote Administrator Agent 6.1 (64-bit)
Collection: Applications - Workstations BTS - ESET Remote Administrator Agent (Member Count: 1)
Use default distribution point groups associated to this collection: Disabled
Automatically distribute content for dependencies: Enabled
Success: Deployment Settings
Action: Install
Purpose: Required
Pre-deploy software to the user's primary device: Disabled
Send wake-up packets: Disabled
Allow clients to use a metered Internet connection to download content: Disabled
Success: Application Settings (retrieved from application in software library)
Application Name: ESET Remote Administrator Agent 6.1 (64-bit)
Application Version: 6.1.265.0
Application Deployment Types: Windows Installer (*.msi file)
Success: Scheduling
Time based on: UTC
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

4.4.4 Product installation

ESET security products can be installed remotely by clicking on the desired machine and selecting **New**, or by creating a new **Software Install** task under **Admin** > **Client Tasks** menu. Click **New...** to begin setting up your new task.

- Use following written instructions or watch Knowledgebase instructional video.

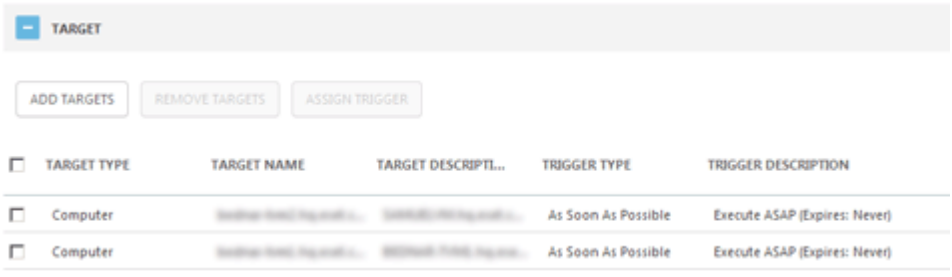


Basic

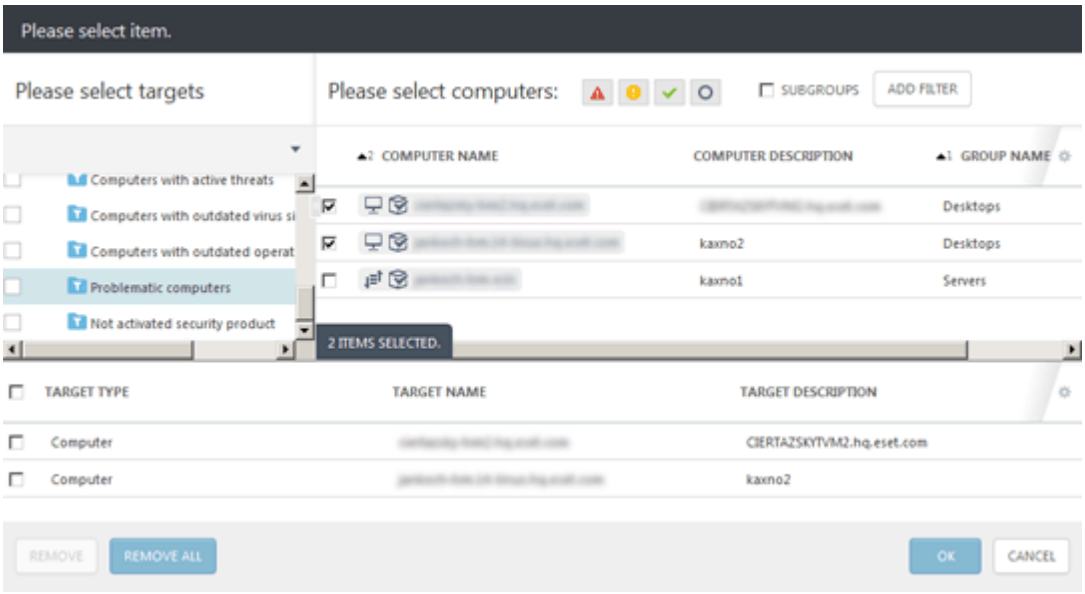
Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. Select the **Software Install** task and then click **Target**.

Target

Here you can specify the clients (individual computers or whole groups) that will receive this task.

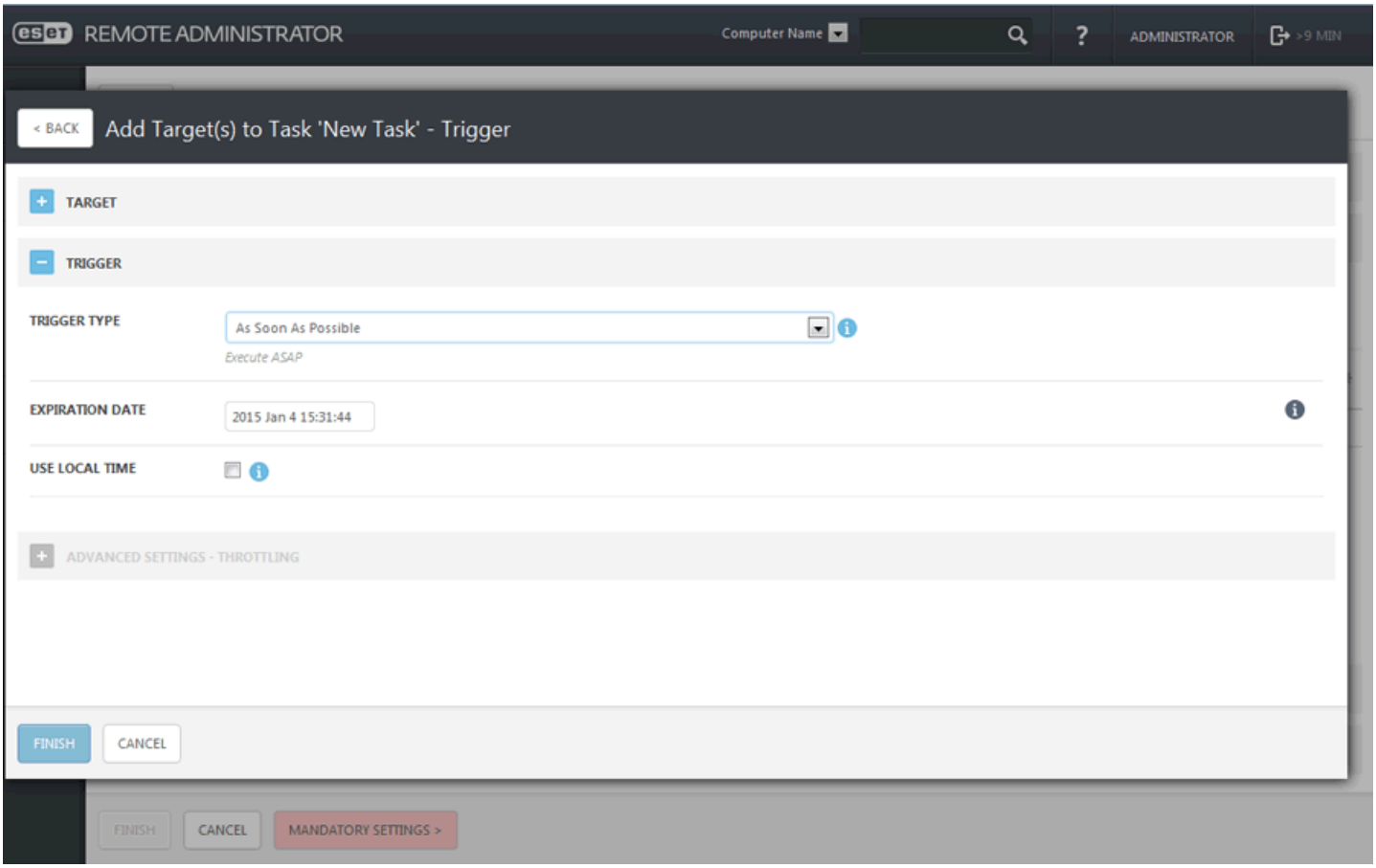


Click **Add targets** to display all Static and Dynamic Groups and their members.



Trigger

As a **Trigger** select **Execute ASAP**, this will send the task to clients immediately. The **Use Local Time** option refers to the local time of the client(s), not the server.



Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For now, we leave Throttling as it is and click **Finish** to create the new task.

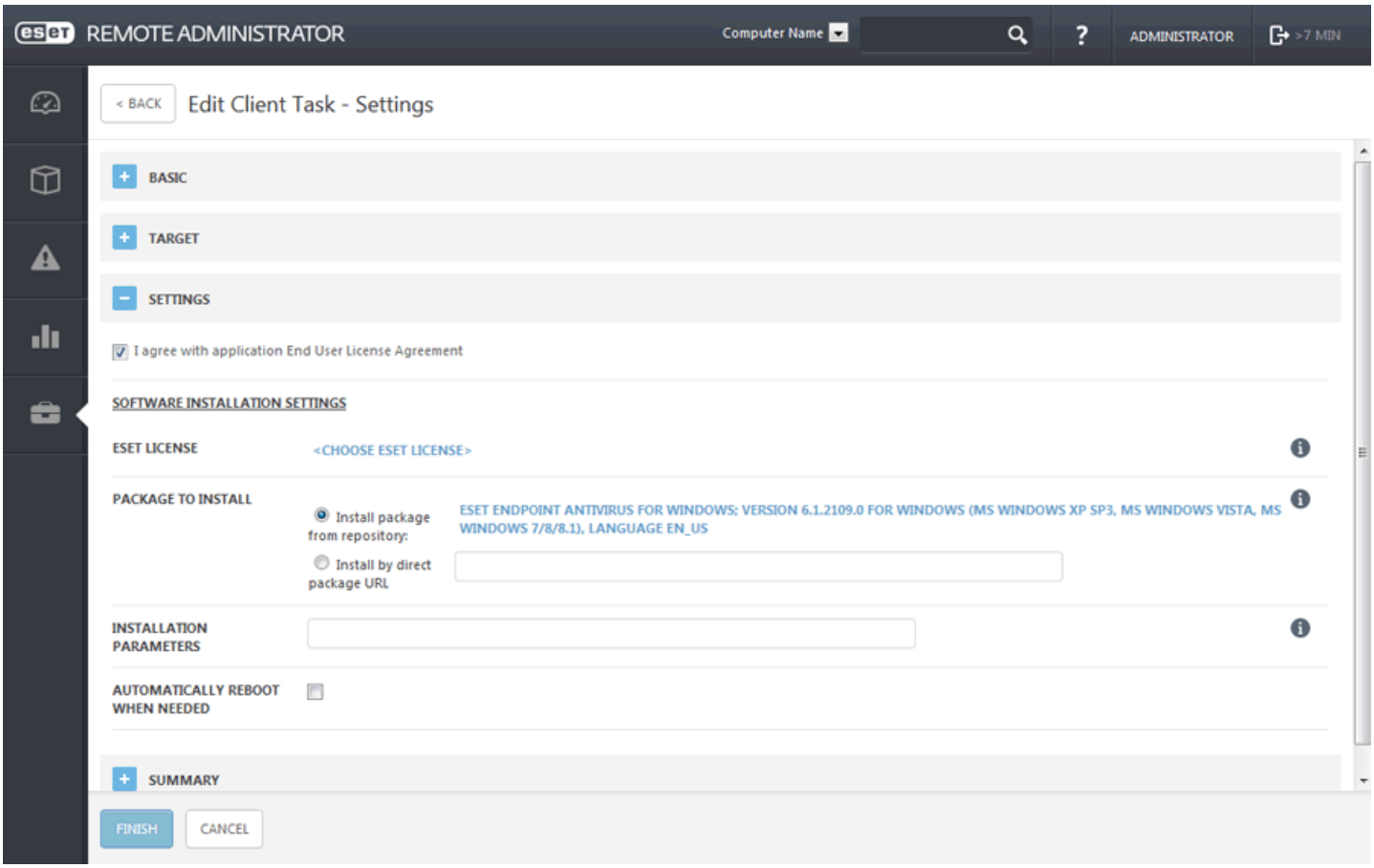
Settings

Click **<Choose ESET License>** and select the appropriate license for the installed product from the list of available licenses. Select the check box next to **I agree with application End User License Agreement** if you agree. See License Management or EULA for more information.

Click **<Choose package>** to select a installer package from the repository or specify a package URL. A list of available packages where you can select the ESET product you want to install (for example, ESET Endpoint Security) will be displayed. Select your desired installer package and click **OK**. If you want to specify installation package URL, type or copy and paste the URL into the text field (do not use URL that requires authentication).

NOTE: Please note, that both Server and Agent needs to have access to the internet, to be able to access the repository and perform the installation. If you do not have internet access, you can install the client software locally.

If you need to, you can specify Installation parameters, otherwise leave this field empty. Select the check box next to **Automatically reboot when needed** to force an automatic reboot of the client computer after installation. Alternatively, you can leave this option unchecked and the decision to restart can be made by someone using the client computer.



Summary

Review the summary of configured settings and click **Finish**. The task is now created and will be sent to the client(s).

4.4.4.1 Product installation (command line)

All the following settings are meant to be used **only with the reduced**, **basic and none** level of the user interface. See documentation for the msiexec version used for the appropriate command line switches.

APPDIR=<path>

- path - Valid directory path
- Application installation directory.

APPDATADIR=<path>

- path - Valid directory path
- Application Data installation directory.

MODULEDIR=<path>

• path - Valid directory path
• Module installation directory.

ADDLOCAL=<list>

• Component installation - list of non-mandatory features to be installed locally.
• see http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx
ees_nt64_ENU.msi /qn ADDLOCAL=<list>

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 - Disabled, 1 - Enabled
• PUA

CFG_LIVEGRID_ENABLED=1/0
• 0 - Disabled, 1 - Enabled
• LiveGrid

CFG_REPORTING_ENABLED=1/0
• 0 - Disabled, 1 - Enabled
• LiveGrid Anonymous Usage Data Reporting

CFG_PCU_UPDATE_MODE=40/36/34
• 34 - Ask, 36 - Always, 40 - Never
• Mode of the Program Component Update.

CFG_FIRSTSCAN_ENABLE=1/0
• 0 - Disable, 1 - Enable
• Schedule a new FirstScan after installation.

CFG_EPFW_MODE=0/1/2/3
• 0 - Automatic, 1 - Interactive, 2 - Policy, 3 - Learning

CFG_PROXY_ENABLED=0/1
• 0 - Disabled, 1 - Enabled

CFG_PROXY_ADDRESS=<ip>
• Proxy IP address.

CFG_PROXY_PORT=<port>
• Proxy port number.

CFG_PROXY_USERNAME=<user>
• username for authentication.

CFG_PROXY_PASSWORD=<pass>
• Password for authentication.

4.4.4.2 List of problems when installation fails

- Installation package not found.
- Required newer version of the Windows Installer Service.
- Another version or conflicting product is already installed.
- Another installation is already in progress. Complete that installation before proceeding with this install.
- Installation or uninstallation finished successfully but computer restart is required.
- Task failed - there was an error, you need to look at the Agent trace log and check the return code of the installer.

4.5 Management

This sections demonstrates how to Add computer or Mobile devices to a groups. How to create new policy and assign a policy to a group.

4.5.1 Add computers to groups

Client computers can be added to groups. This helps you keep the computers structured and arranged to your liking. You can add computers to either a Static or Dynamic Group.

Static Groups are managed manually and Dynamic Groups are arranged automatically based on specific criteria in a template. Once the computers are in groups, you can assign policies, tasks or settings to these groups. The policy, task or setting is then applied to all the members of the group. The correlation between groups and tasks/policies is described here:

Static Groups

Static Groups are groups of manually selected and configured clients. Their members are static and can only be added/removed manually, not based on dynamic criteria.

Dynamic Groups

Dynamic Groups are groups of clients where membership in the group is determined by specific criteria. If a client does not meet the criteria, it will be removed from the group. Computers that meet the criteria will be added to the group automatically - hence the name Dynamic.

4.5.1.1 Static groups

- Static Groups are used to manually sort client computers into **groups** and **subgroups**. You can create custom Static Groups and move desired computers into them.
- Static Groups can be created only manually. Client computers can then be moved manually into these groups. Each computer can belong only to one Static Group.

There are two default Static Groups:

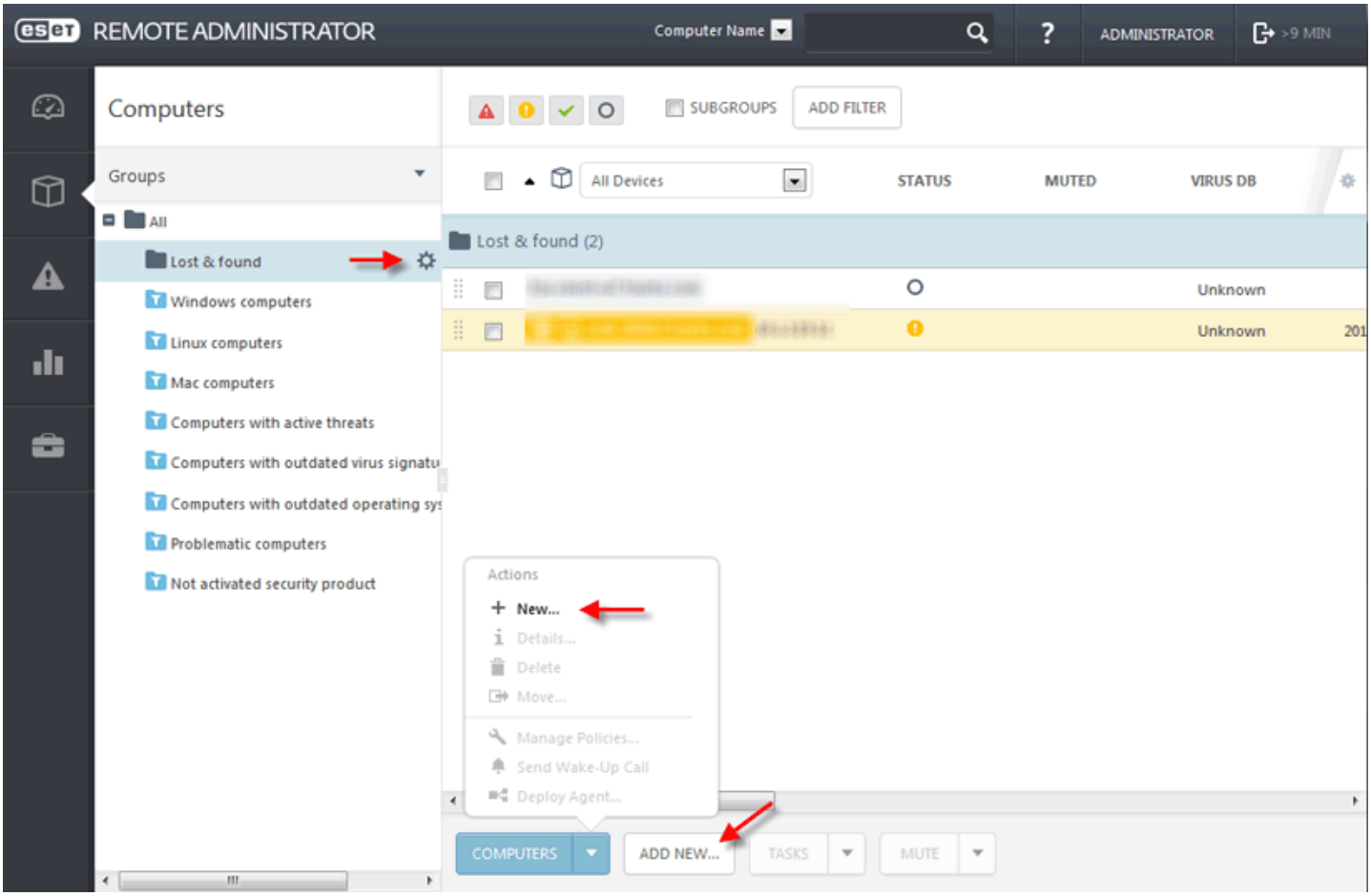
- **All -** This is a main group for all computers in ERA Servers network. It is used for applying of Policies for each computer as a default policy. The group is always displayed and it is not allowed to change Groups name by editing the group.
- **Lost & Found** as a child group of group **All** - Each new computer that first time connects with Agent to server is automatically displayed in this group. The group can be renamed, copied but it can't be deleted or moved.

You can create Static Groups in the **Group** section of the **Admin** tab by clicking the Groups button and selecting New Static Group.

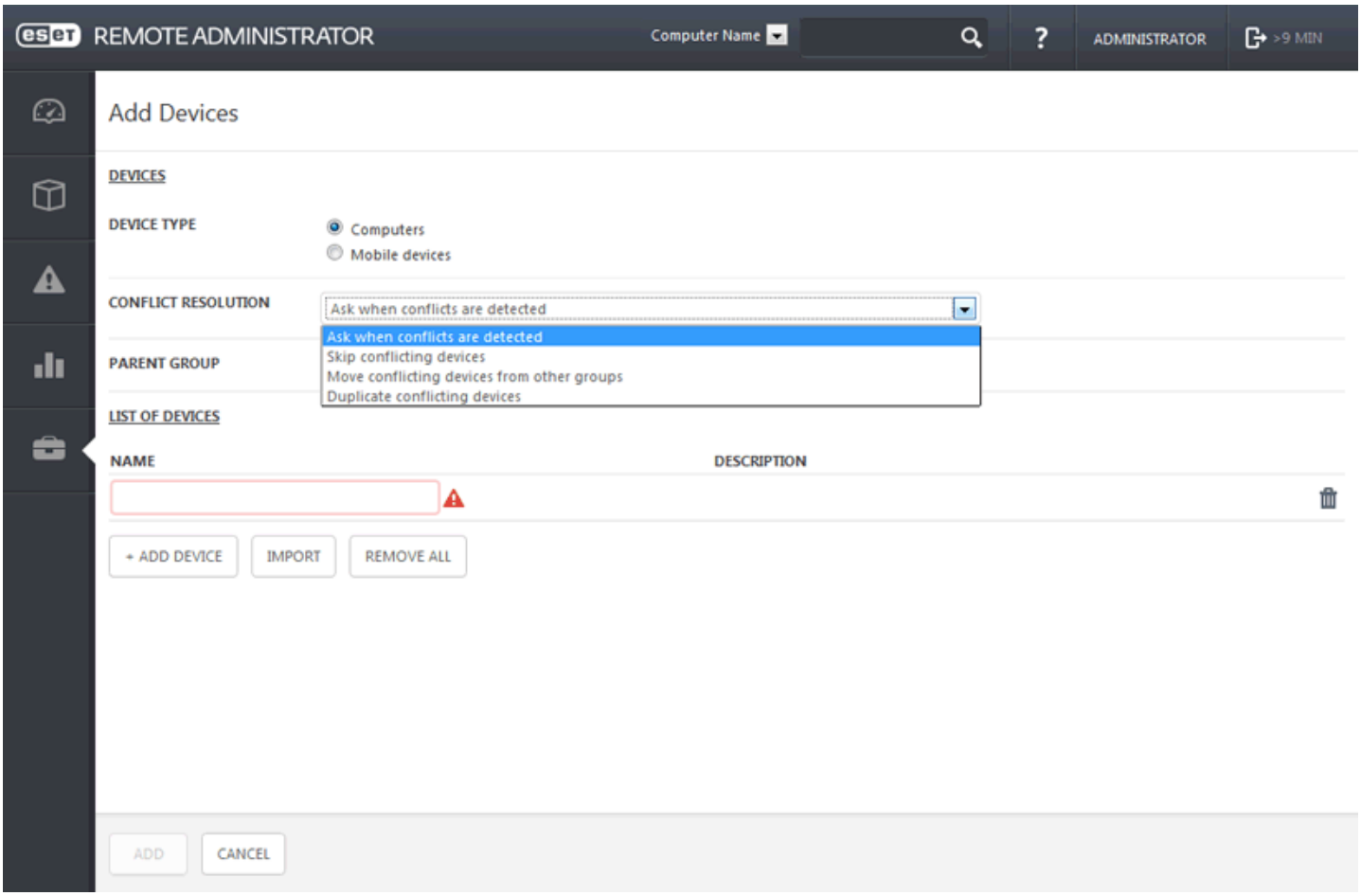
4.5.1.1.1 Add computer to a static group

Create New Static Group or select one of the default Static Groups.

From the **Computers** tab there are three ways to add new computers. For example, select a Static Group, click the cogwheel icon and select + **Add New**.



Type the name of the computer you want to add into the **Name** field. Click + **Add Device** to add additional computers or click Import to import a file with a list of computers to add. Optionally, you can enter a **description** of the computers.



Use the **Conflict Resolution** drop-down menu to select the action to take if a computer you are adding already exists in ERA:

Ask when conflicts are detected: When a conflict is detected, the program will ask you to select an action (see the options below).
Skip conflicting computers: Duplicate computers will not be added.
Move conflicting computers from other groups: Conflicting computers will be moved from their original groups to the **All** group.
Duplicate conflicting computers: New computers will be added, but with different names.

Click **Add**. Computers can be viewed in the list on the right when you select the group they belong to.

NOTE: Adding multiple computers may take a longer time, reverse DNS lookup may be preformed.

For more information how to add Mobile devices see chapter Mobile device enrollment.

4.5.1.2 Dynamic groups

Every Dynamic Group uses a Template to filter client computers. Once defined, a template can be used in other Dynamic Group to filter clients. ERA includes several default Dynamic Group templates out-of-the box to make it easy to categorize client computers.

Dynamic Groups are groups of clients selected based on specific criteria. If a client computer does not fulfill the criteria, it will be removed from the group. if it fulfills the defined conditions, it will be added to the group. Group selection happens automatically based on configured settings, except for in the case of Static Groups.

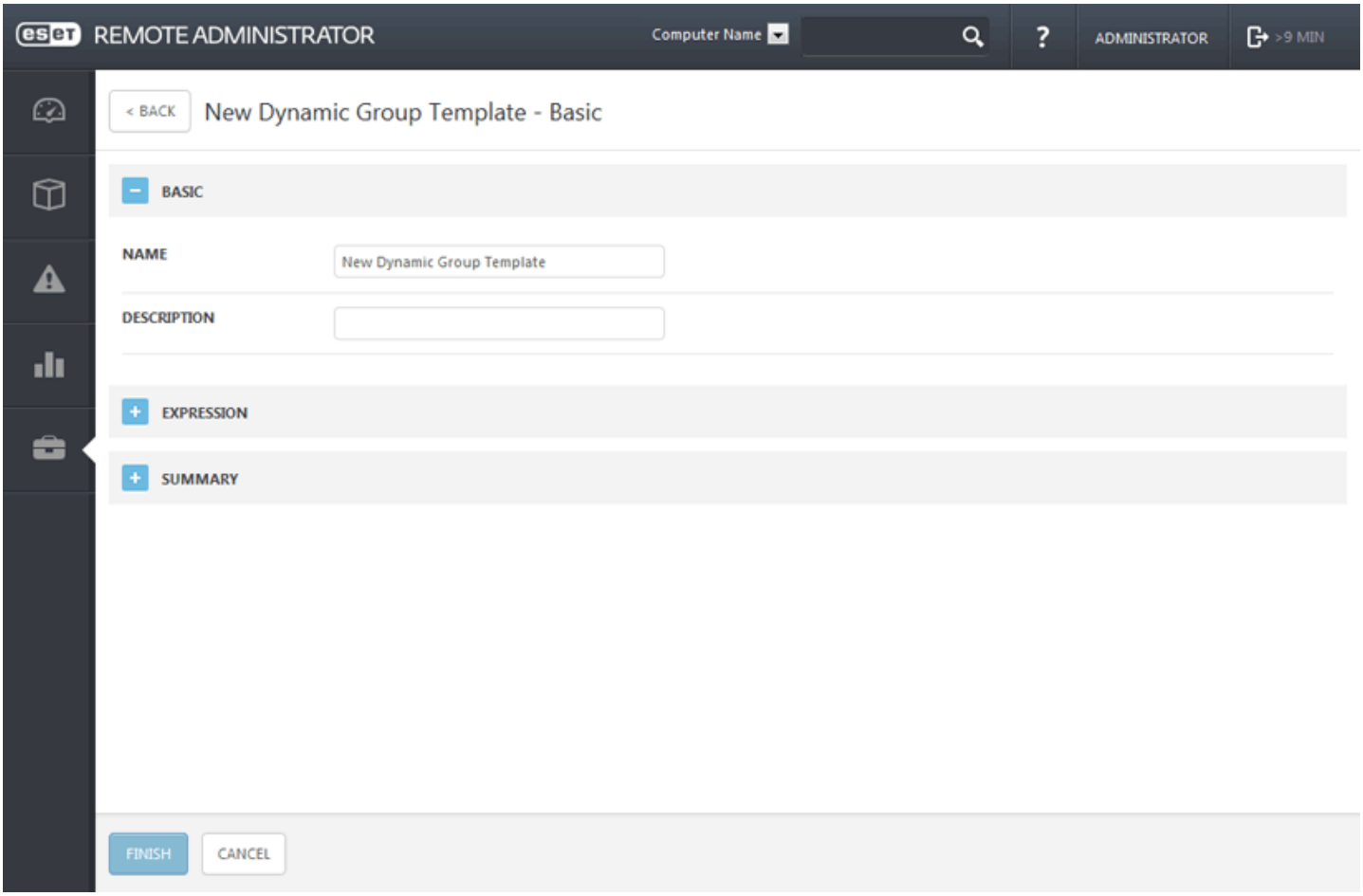
The Dynamic Group Templates section contains both pre-defined and custom templates based on different criteria. All templates are displayed in a list. Clicking an existing template allows you to edit it. To create a New Dynamic Group template, click **New Template**.

4.5.1.2.1 New Dynamic Group Template

Click **New Template** under **Admin** > **Dynamic Group Templates.**

Basic

1. Enter a **Name** and a **Description** for the new Dynamic Group template.



Expression

Select a logical operator in the **Operation** menu.

- **AND** - All defined conditions have to be true.
- **OR** - At least one condition has to be true.
- **NAND** - At least one condition has to be false.
- **NOR** - All conditions have to be false.

For example, select **AND**. This means that a computer must meet all conditions in order to appear in a Dynamic Group that uses this template.

- Click **+ Add Rule** and select a condition. Let's say you aim at clients who use laptops that are plugged into electricity. Select **Hardware** > **Running on battery** > **=(equal)** > **Not discharging**.
- Click **+ Add Rule** to enter a second condition (number of rules is not limited). Select **OS edition** > **OS type** > **=(equal)** > **Windows 8.1** (enter this value into the blank field).

If both of these conditions are met, the client will appear in the Dynamic Group.

Summary

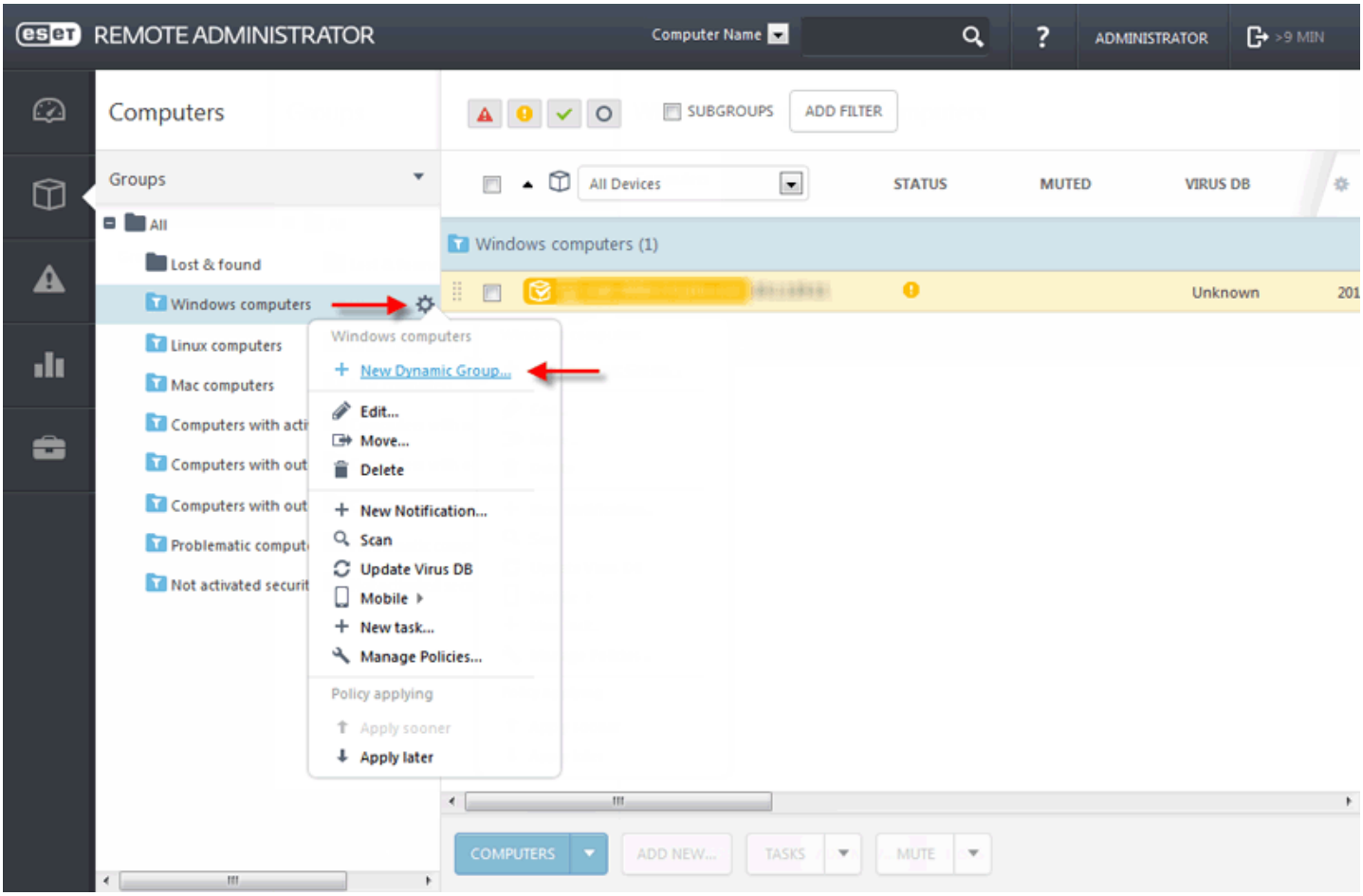
Review the configured settings and click **Finish** to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.In **Expression** options you can configure rules/conditions for the group (Rule editor is described here). Now, every Dynamic Group based on this template will evaluate these rules.

To save your changes, click **Finish**.

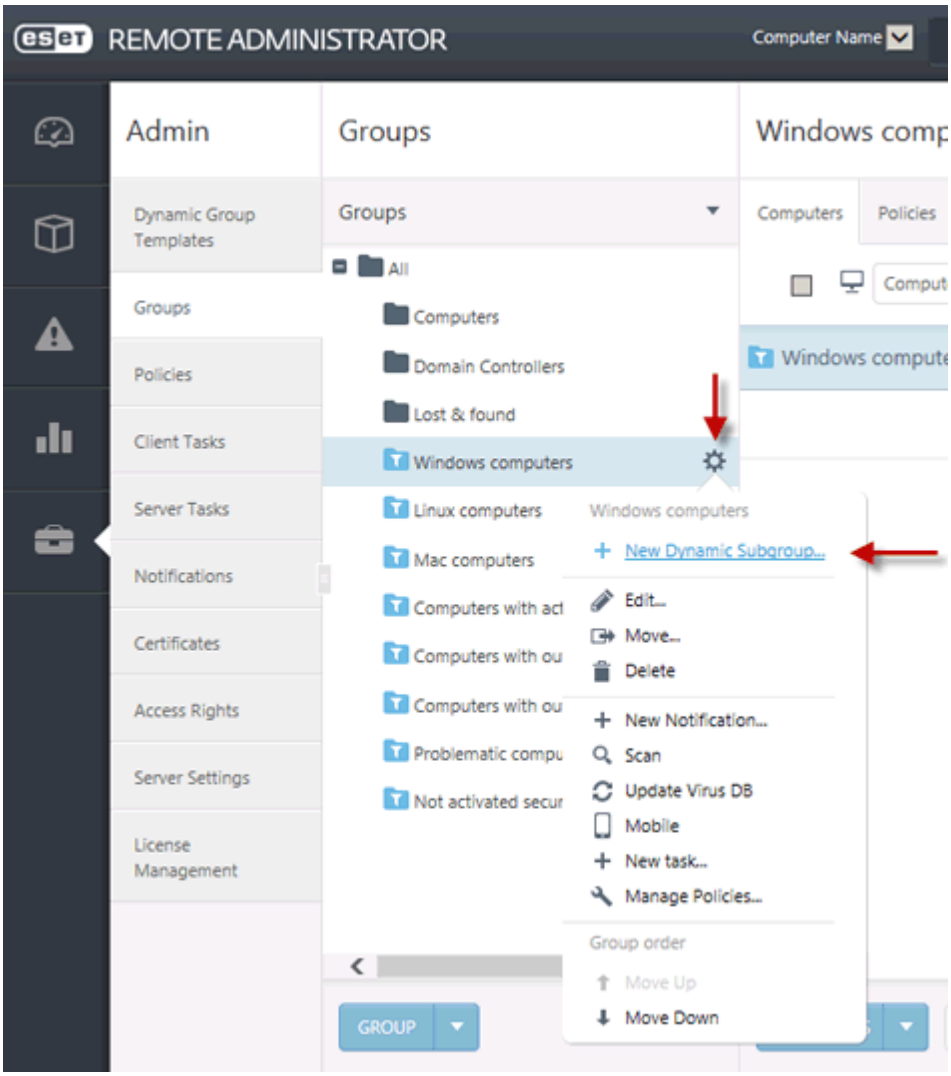
4.5.1.2.2 Create new Dynamic Group

There are three ways to create a New Dynamic Group:

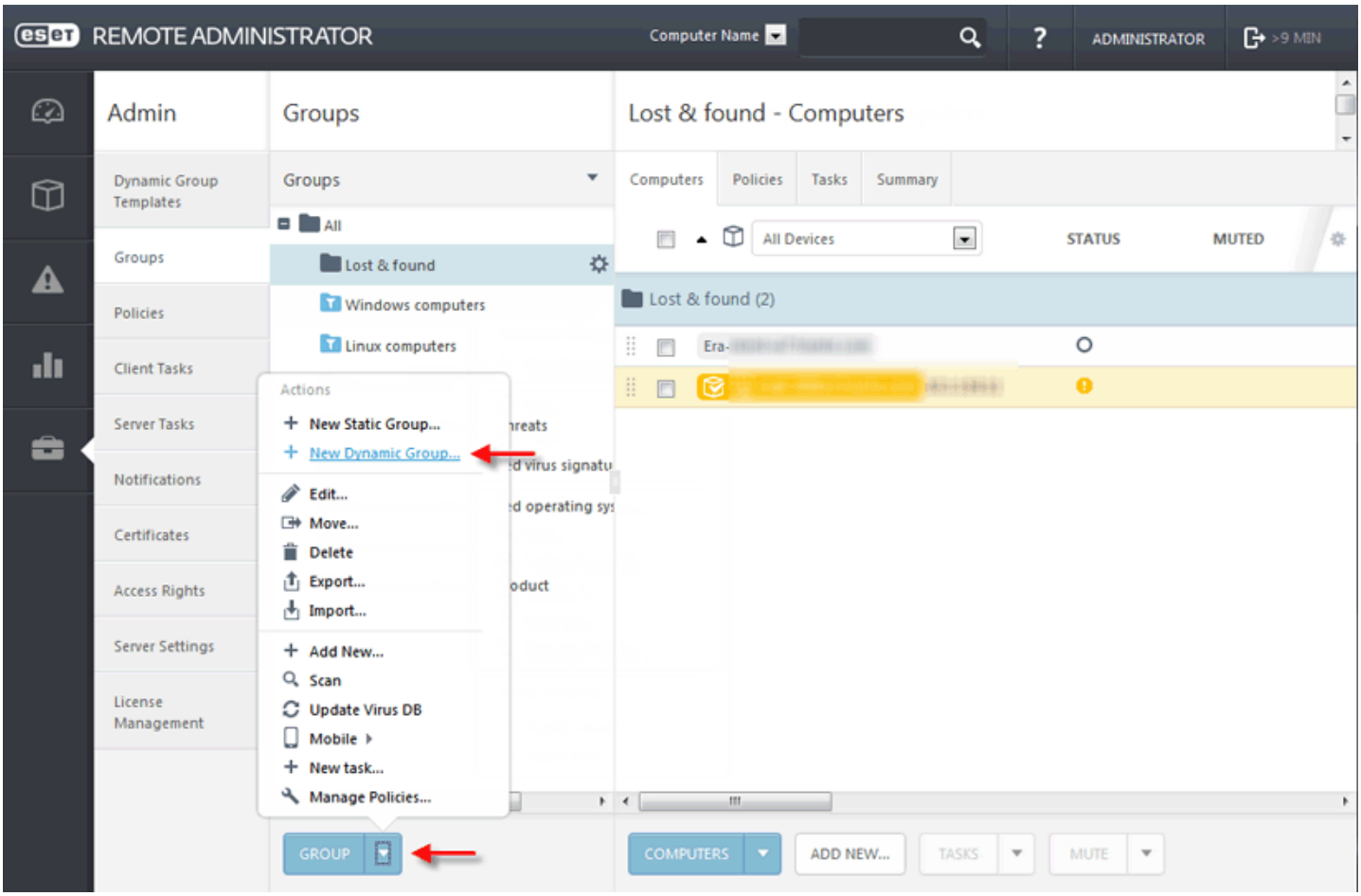
1. Click **Computers** > **Groups** > ⚙ and select **New Dynamic Group...**



2. Click **Admin** > **Groups** > ⚙ > **New Dynamic Subgroup...**



3. Click **Admin** > **Groups** > Click the **Group** button and click **New Dynamic Group...**



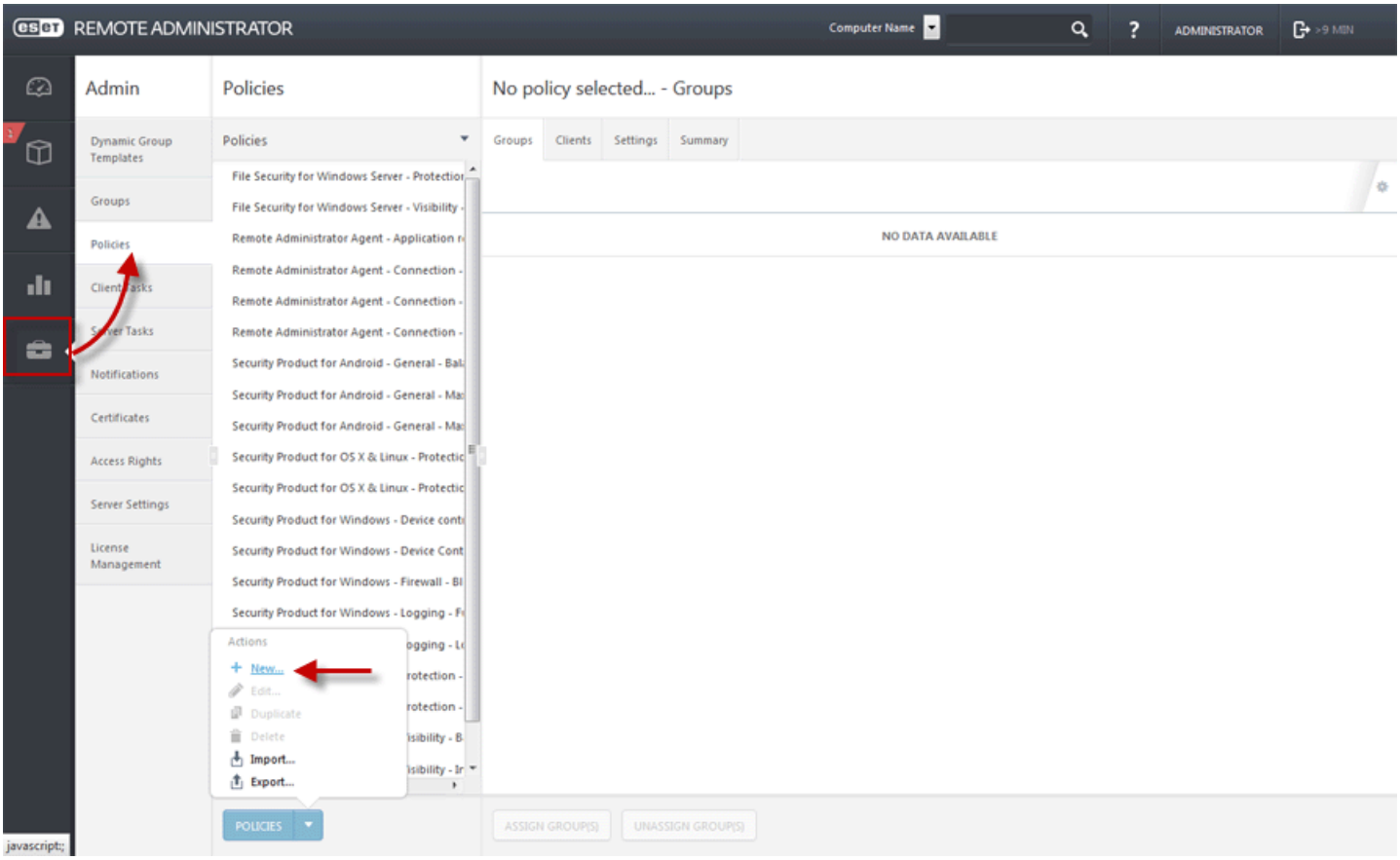
A New Dynamic Group Wizard will appear.

4.5.2 Create a new policy

In this example, we are going to create a new policy for the ERA Agent Connection Interval. We highly recommend doing this prior to testing mass deployment in your environment.

1. Create a New Static Group.

2. Add a new policy by clicking **Admin** > **Policies**. Click **Policies** at the bottom and select **New**.

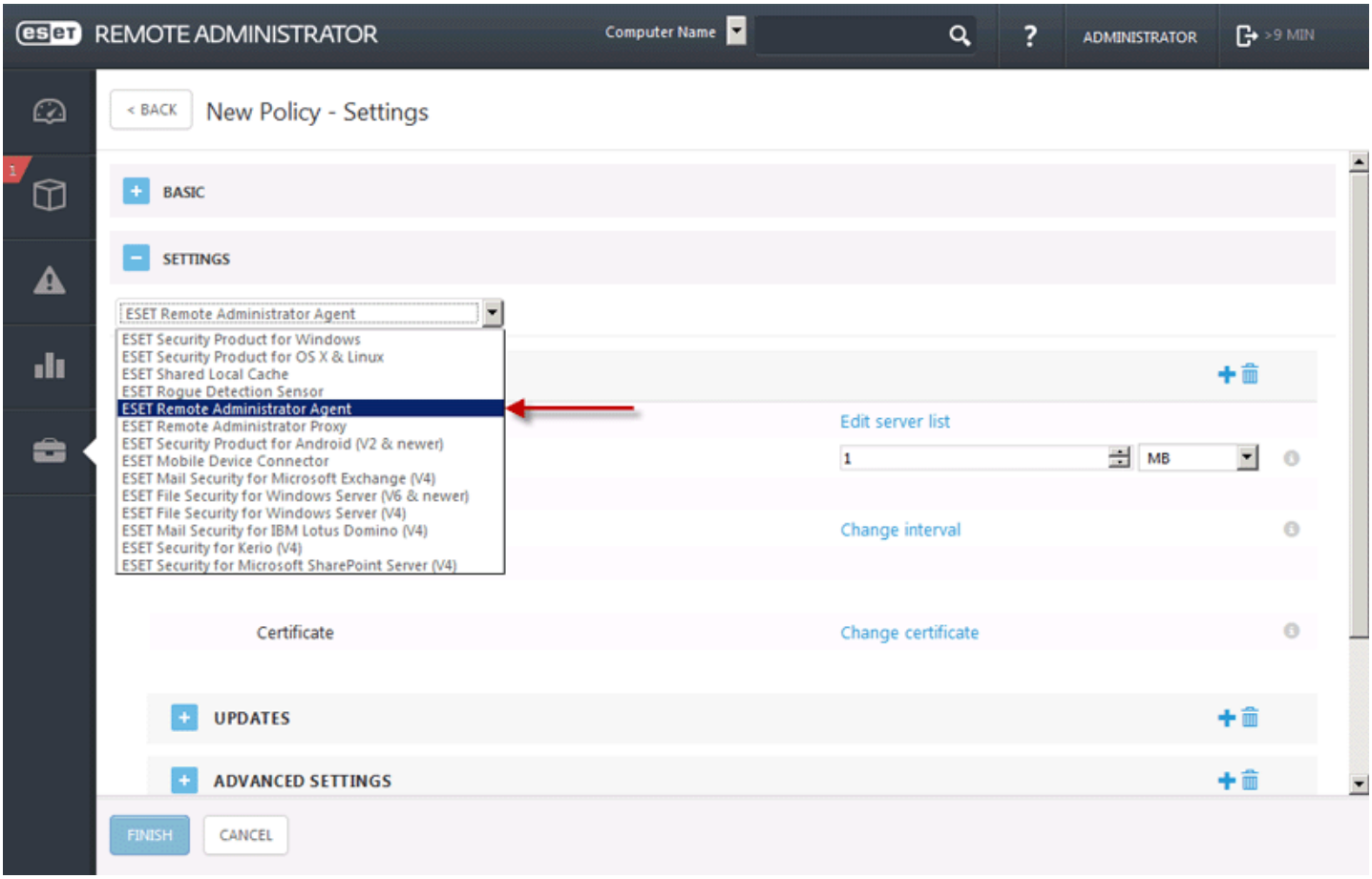


Basic

Enter a **Name** for the new policy (for example "Agent Connection Interval"). The **Description** field is optional.

Settings

Select **ESET Remote Administrator Agent** from the **Product** drop-down menu.



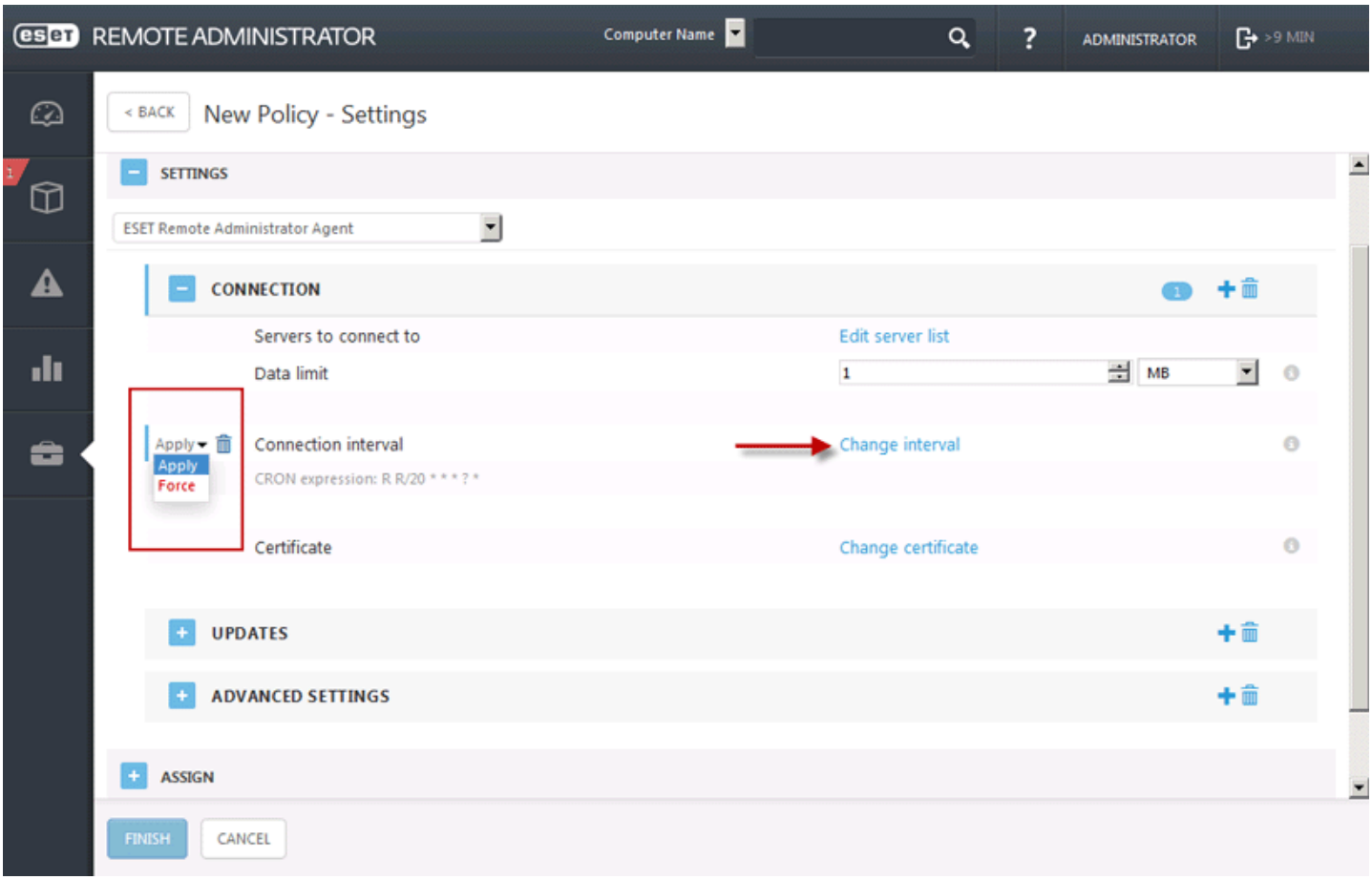
Connection

Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a flag. To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to a category name in the tree on the left. This shows a sum of rules in all its sections. This way, you'll quickly see where and how many settings/rules are defined.

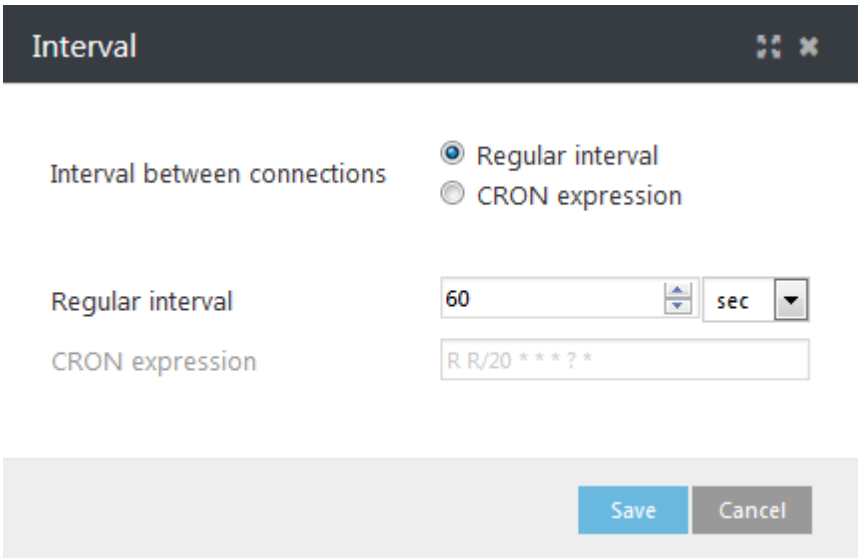
You can also use these suggestions to make policy editing easier:

- use + to set **Apply** flag to all item in current a section
- delete rules using **Trashcan** icon

Click **Change interval**.



In the **Regular interval** field, change the value to your preferred interval time (we recommend 60 seconds) and click **Save**.



Once you've created a new Agent Connection Interval policy, assign it to the Static Group you created in step 1.

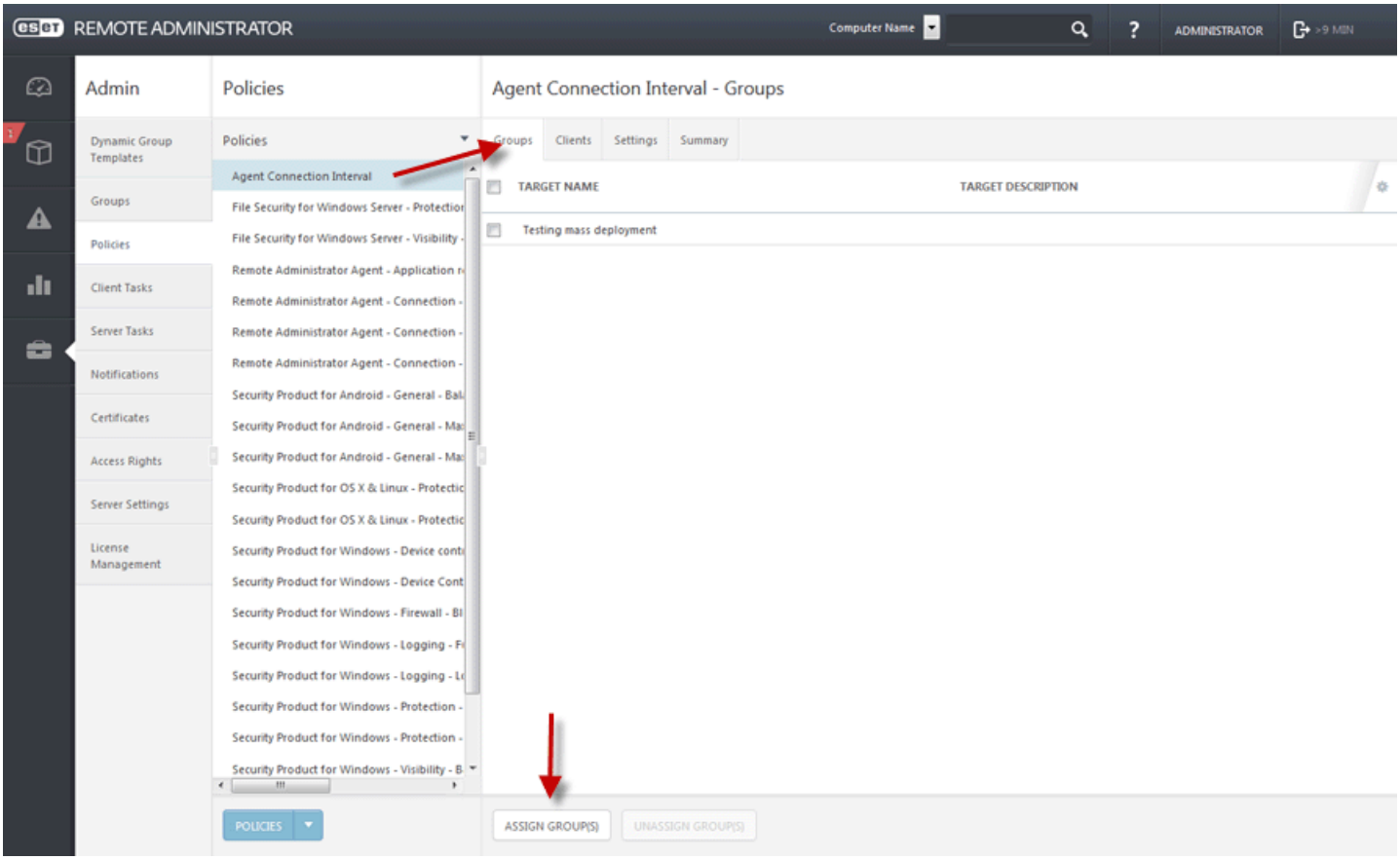
After you are finished with mass deployment testing, edit the ERA Agent Connection Interval policy settings you created in step 2.

Click **Admin** > **Groups** and select the **Policies** tab. Click **Agent Connection Interval policy**, choose **Edit** and then click **Settings** > **Connection**. Click **Change Interval** and set the connection interval to 20 minutes.

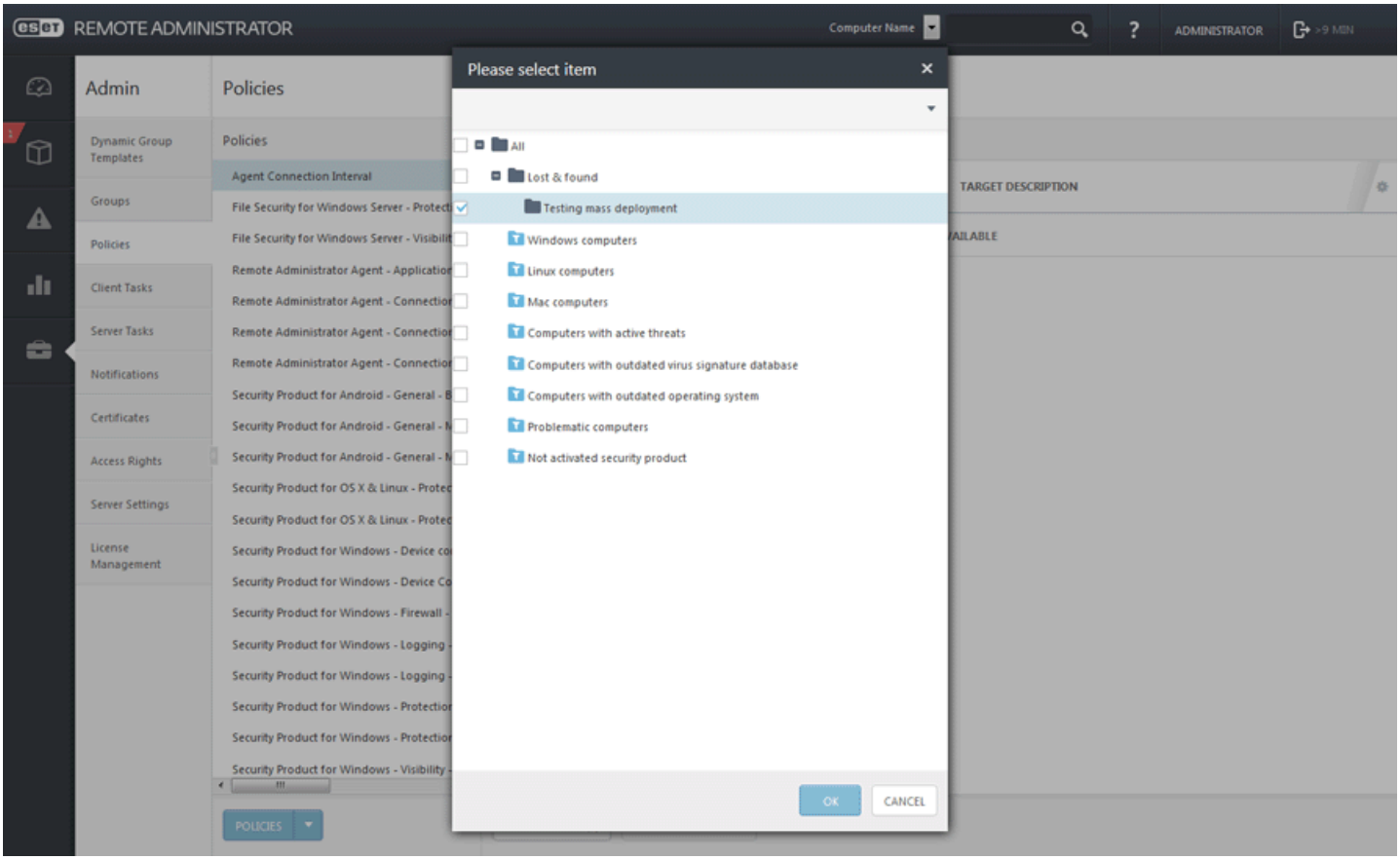
4.5.3 Assign a policy to a group

After a Policy is created, you can assign it to a **Static** or **Dynamic Group**. There are a two ways to assign a policy:

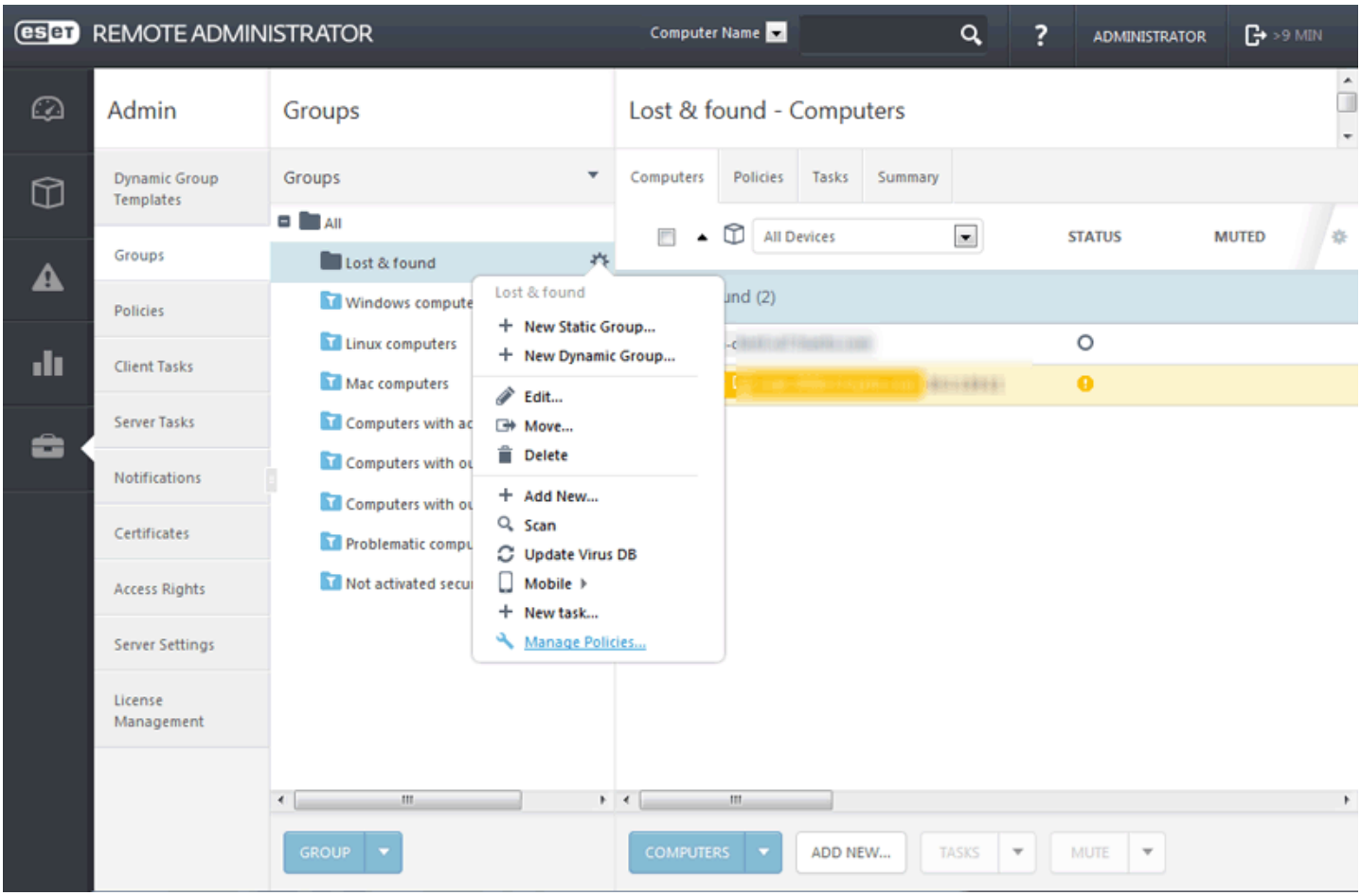
1. Under **Admin** > **Policies** > select a policy and click **Assign Group(s)**. Select a Static or Dynamic Group and click **OK**.



Select **Group** from the list.



2. Click **Admin** > **Groups** > **Group** or click the cogwheel icon next to the group name and select **Manage Policies**.



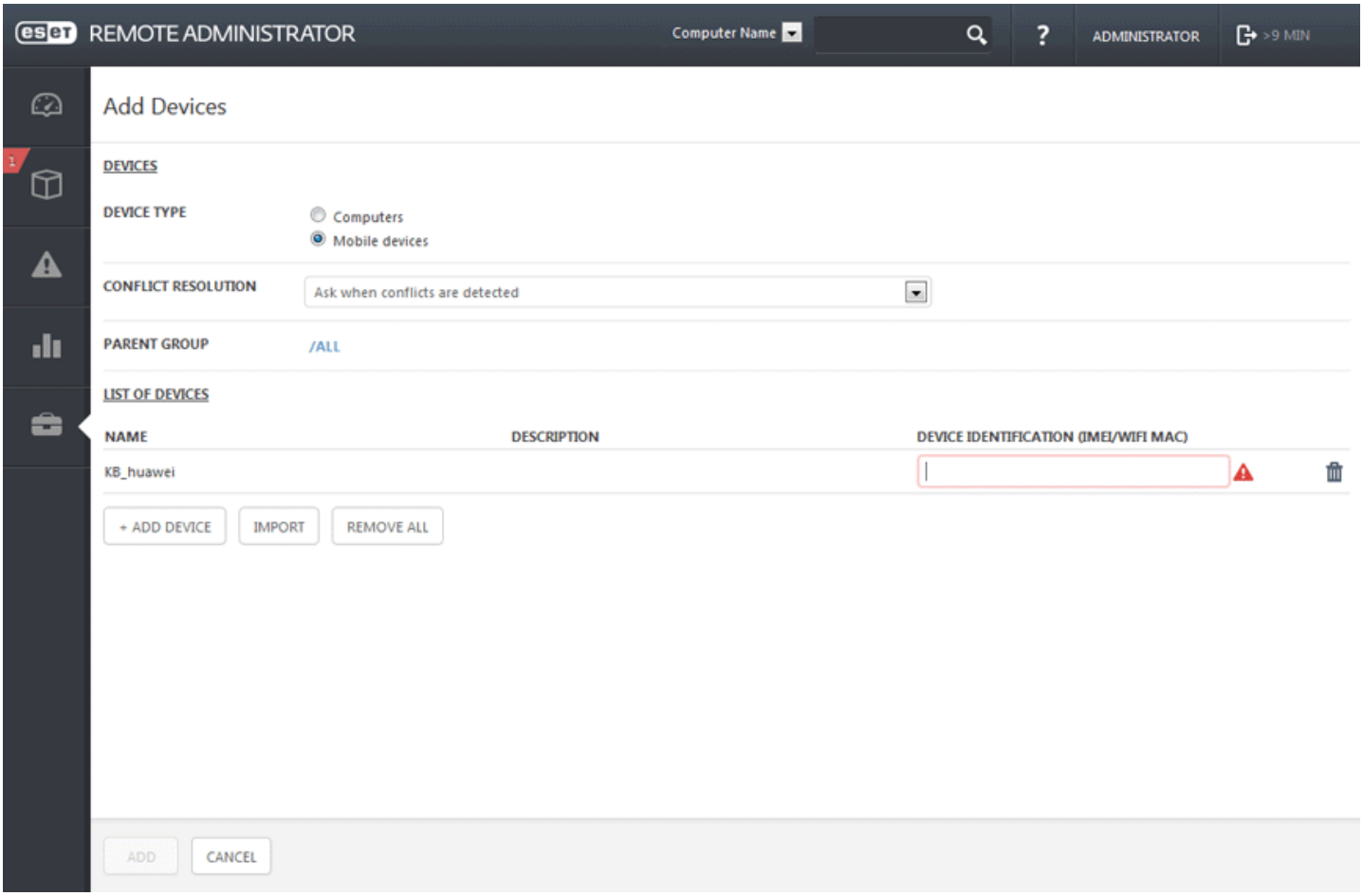
In the **Policy application order** window click **Add Policy**. Select the check box next to the policy that you want to assign to this group and click **OK**.
Click **Save**. To see what policies are assigned to a particular group, select that group and click the **Policies** tab to view a list of policies assigned to the group.

NOTE: For more information about policies, see the Policies chapter.

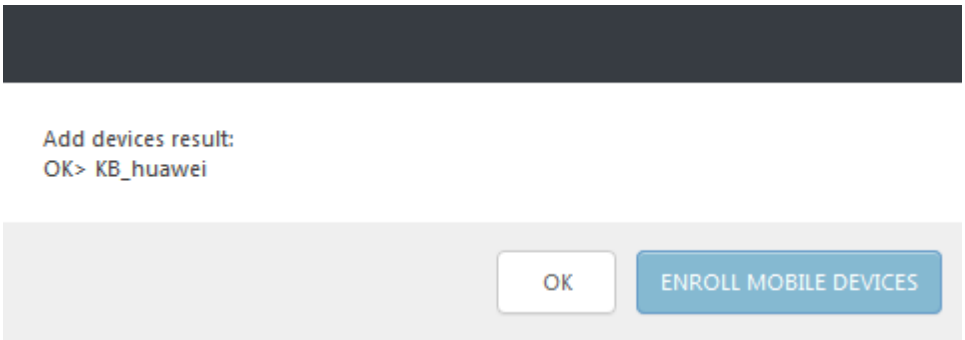
4.5.4 Mobile Device enrollment

You can add Mobile devices to your ERA structure similarly to the way you would add a new computer. To do so, follow the steps below:

1. Click **Admin** > select the Static Group you want to add the mobile device to and click **New...**
2. Select **Mobile devices** and enter a **Name**, **Description** (optional) and **Device Identification** number. Device identification numbers can be an IMEI number (GSM networks), MEID number (CDMA networks) or WiFi MAC address (for WiFi-only mobile devices).



3. There are two ways to enroll a mobile device:
   a. The administrator obtains the MAC address in advance from the device and enrolls the device via ERA the usual way
   b. The user clicks an enrollment link (sent by the administrator). The app will automatically reply that this device is not whitelisted/approved and show the MAC address on the screen–prompting the user to contact the administrator and provide him with the device ID (MAC address).
4. Click **Add** and then click **Enroll Mobile Devices** in the dialog window.



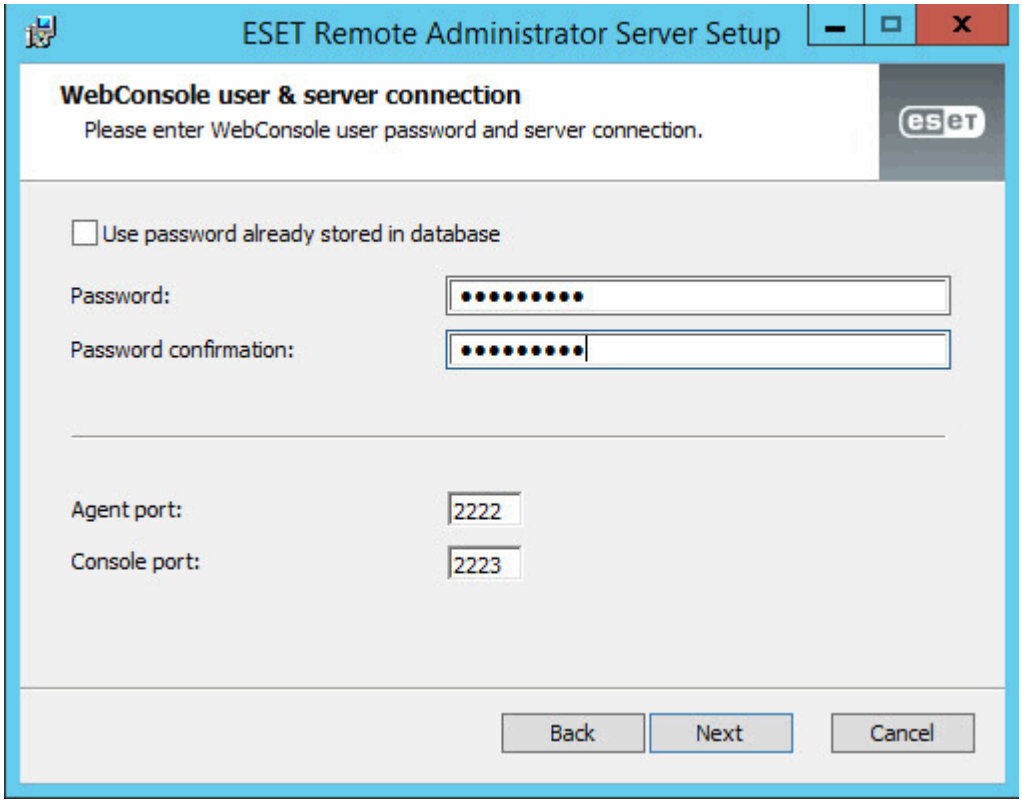
The Device Enrollment task wizard will guide you through the process of Mobile Device Enrollment.

4.6 Best practices

Forgotten password: Ideally, the administrator account should only be used to create accounts for individual admins. Once admin accounts are created, the administrator password should be saved and the administrator account should not be used. This practice allows the administrator account to be used to reset passwords/account details of individual admins should it become necessary.

How to **reset password** of a built-in ERA Administrator account:

- open **Programs and Features** (run appwiz.cpl), locate ESET Remote Administrator Server and right-click it
- select **Change** from the context menu
- choose **Repair**
- specify database connection details
- select **Use existing database** and apply upgrade
- make sure to deselect **Use password already Stored in database** option and enter new password.
- you can now login to the ERA Web Console with your new password



4.6.1 User Management

It is strongly advised that you create additional accounts with specific access rights based on your desired account competencies.

5. Working with ESET Remote Administrator

All clients are managed through the **ERA Web Console**. You can access the Web Console from any device using a compatible browser. The Web Console is divided into three main sections:

1. At the top of the Web Console, you can use the **Quick Search** tool. Type a **Client name** or **IPv4/IPv6 Address** and click the magnifier symbol or press **Enter**. You will be redirected to the Groups section where the relevant client(s) will be displayed.

2. The menu on the left contains the main sections of ESET Remote Administrator and the following Quick links:

- Dashboard
- Computers
- Threats
- Reports
- Admin

Quick links

- New Native User
- New Policy
- New Client Task
- Agent Live Installers

3. Buttons on the bottom of the page are unique for each section and function, and are described in detail in their respective chapters.

NOTE: One button is common for all new items - **Mandatory Settings**. This red button is displayed when mandatory settings have not been configured and therefore creation can not continue. This is also indicated by a red exclamation mark next to each section. Click **Mandatory Settings** to navigate to the section where the settings in question are located.

General rules

- Required (mandatory) settings are always marked with a red exclamation mark next to the section and the respective settings. To navigate to mandatory settings (if applicable), click **Mandatory settings** at the bottom of each page.
- If you need help when working with ESET Remote Administrator, click the **?** icon in the top right corner or navigate to the bottom of the pane on the left and click **Help**. The respective help window for the current page will be displayed.
- The **Admin** section is for specific configuration, read the Admin chapter for more information.

5.1 Dashboard

Dashboard is the default page that is displayed after the user logs into the ERA Web Console for the first time. It displays pre-defined reports about your network. You can switch between dashboards using the tabs in the top menu bar. Each dashboard consists of several reports. You can customize your dashboards by adding reports, modifying existing ones, resizing, moving and re-arranging them. All this gives you a comprehensive overview of ESET Remote Administrator and its parts (clients, groups, tasks, policies, users, competences, etc.). Four dashboards come pre-configured in ESET Remote Administrator:

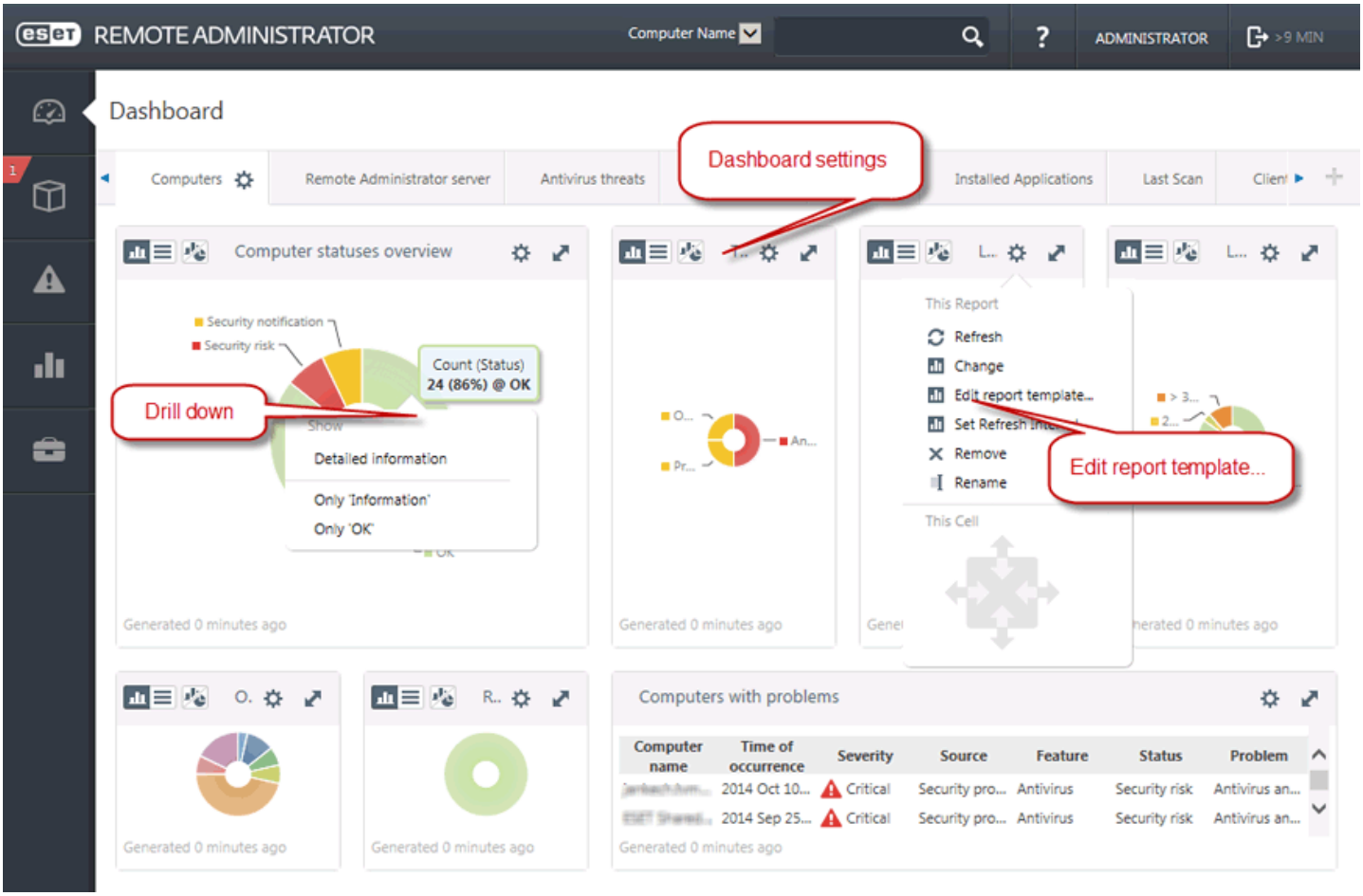
Computers
This dashboard gives you an overview of client machines - their protection status, operating systems, update status, etc.

Remote Administrator Server
In this dashboard, you can view information about the ESET Remote Administrator server itself - server load, clients with problems, CPU load, database connections, etc.

Antivirus threats
Here you can see reports from the antivirus module of the client security products - active threats, threats in the last 7/30 days and so on.

Firewall threats
Firewall events of the connected clients - according to their severity, time of reporting, etc.

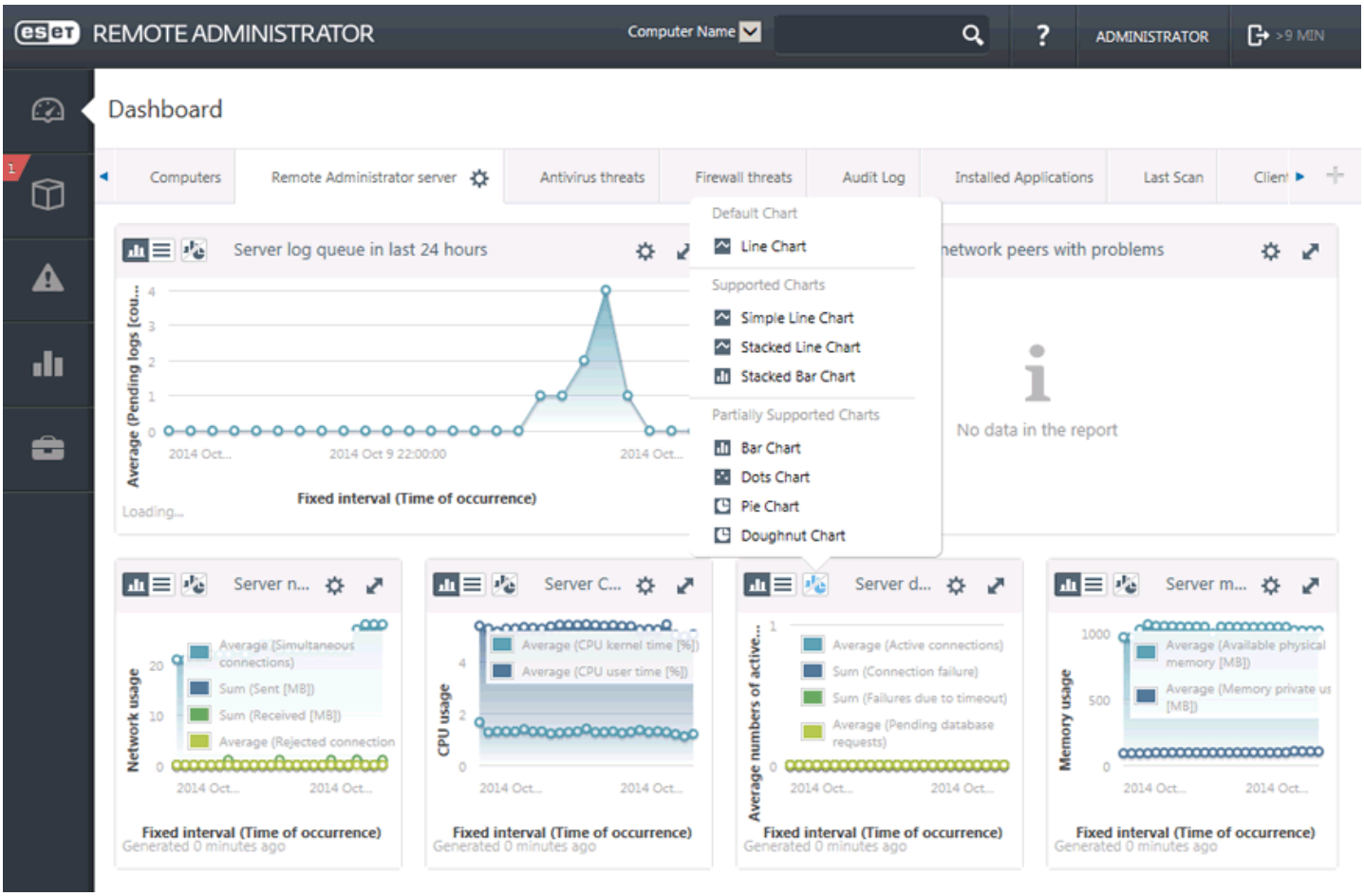
Dashboard functionality:



5.1.1 Dashboard settings

Dashboard settings are available for all dashboards, pre-defined and newly created, and let you manage your dashboards. The available options are described below:

- **Add a new dashboard** - Click the + symbol on the top of the Dashboard header. Enter a name for the new Dashboard and click **OK** to confirm. A new Dashboard with nothing in the reports field is created. Once you set up your dashboard, you can start adding reports to it.
- **Duplicate a dashboard** - Select the Dashboard you want to duplicate and click the **cogwheel** ⚙ symbol next to the Dashboard name. Select **Duplicate** from the list - a duplicated Dashboard is created.
- **Move a dashboard** - Click and drag the name of a dashboard to change its location relative to other dashboards.
- **Change the dashboard size (number of reports displayed)** - Click the **cogwheel** ⚙ symbol > **Change layout**. Select the number of reports you want to display in the dashboard (drag) and click them. The dashboard layout will change.
- **Rename a dashboard** - Click the **cogwheel** ⚙ symbol next to the Dashboard name and click **Rename**. Enter a new name for the Dashboard and click **OK**.
- **Remove a dashboard** - Click the **cogwheel** ⚙ symbol next to the Dashboard name, click **Remove** and then confirm the removal.
- **Resize** click the **double-arrow** symbol at the right of a report to re-size it. More relevant reports are larger, while less relevant reports are smaller, you can also toggle full screen mode to display any report full-screen.



- **Change Chart Type-** click the **Chart** symbol at the top left corner of a chart and select **Pie Chart**, **Line Chart** etc. to change the chart type.
- Click **Refresh** to refresh the displayed information.
- Click **Change** to view a different report.
- Click Edit report template to add or edit a template.
- Click **Set Refresh interval** to define how often the data in a report is refreshed. **The default refresh interval is 120 seconds**.
- **Rename/Remove** the report.

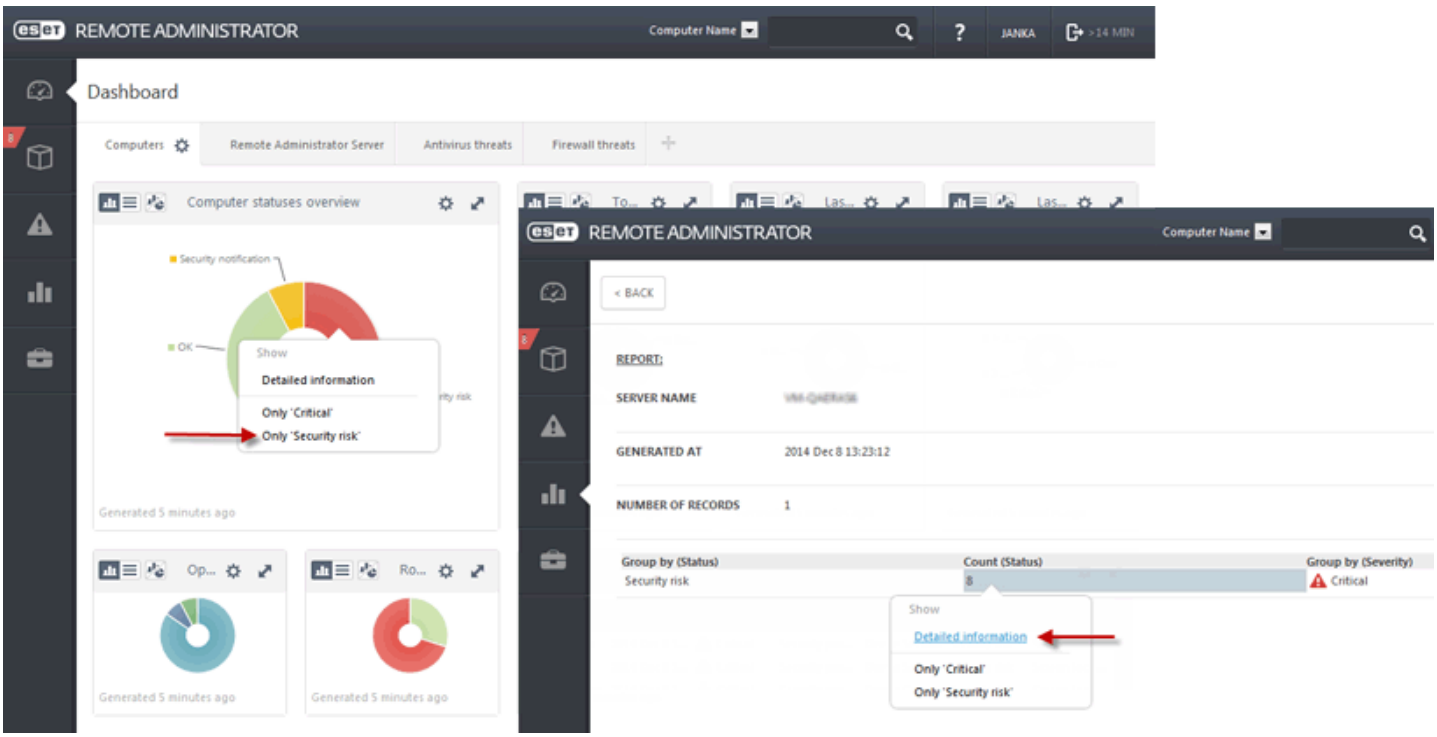
5.1.2 Drill down

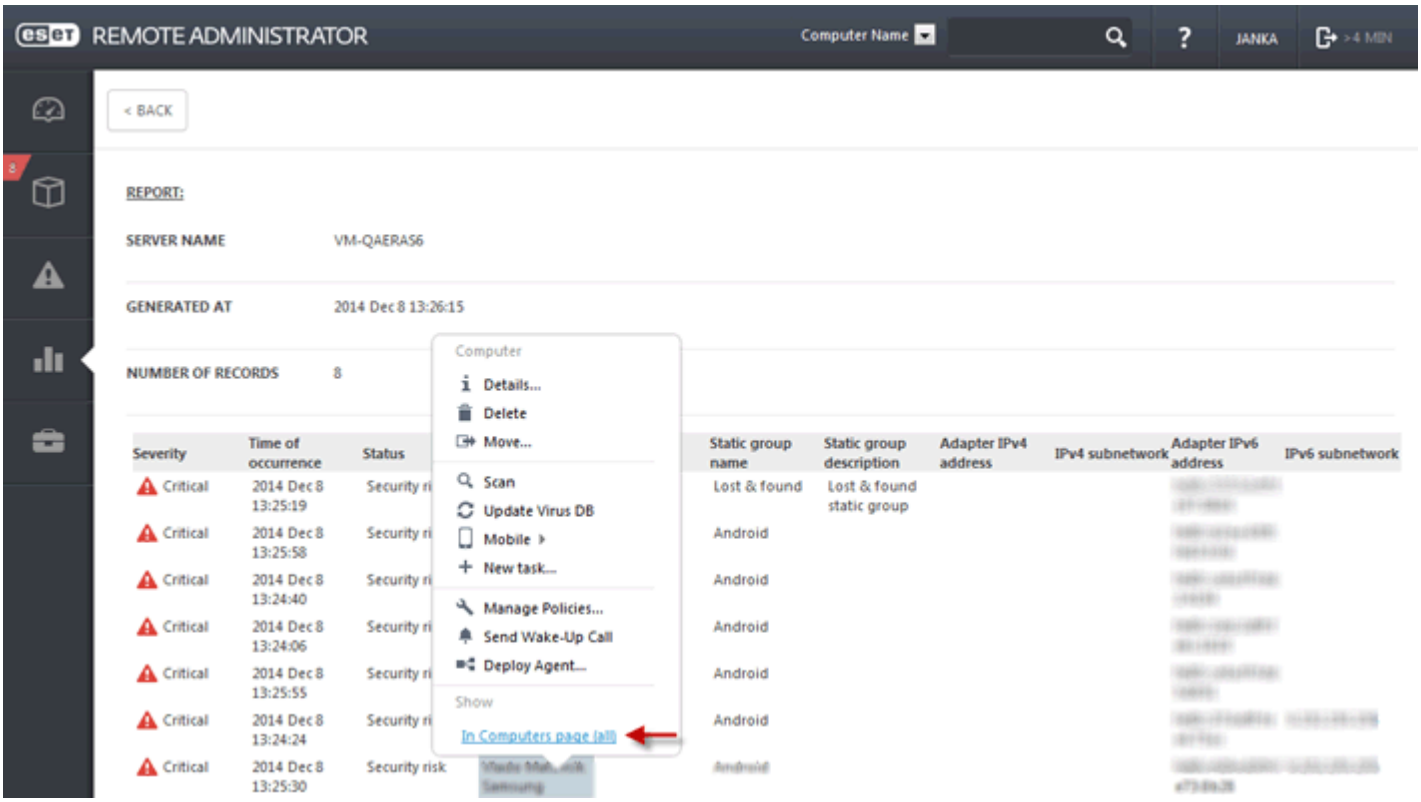
This Dashboard functionality is useful for data examination in greater detail, it lets you interactively select specific items from a summary and view detailed data about them. Focus in on the item of interest by 'drilling down' from summary information in order to get further information about this particular item. There are usually multiple levels you can drill down through.

There are four drill down types:

- Show **Detailed information** - computer name and description, Static Group name etc. Displays original (not aggregate) data for the clicked row.
- Show **Only '***value***'** - Information, Critical, Security risk, Security notification etc.
- **Expand column '***value***'** - it will show aggregated information (usually for count or sum), for example if there is just a number in the column and you click **Expand column Computer**, it will list all details about computers
- Show **In Computers page (all)** - redirects you to the Computers page (shows a result of 100 items only)

NOTE: The results you get using drill down of other reports will show the first 1000 items only.

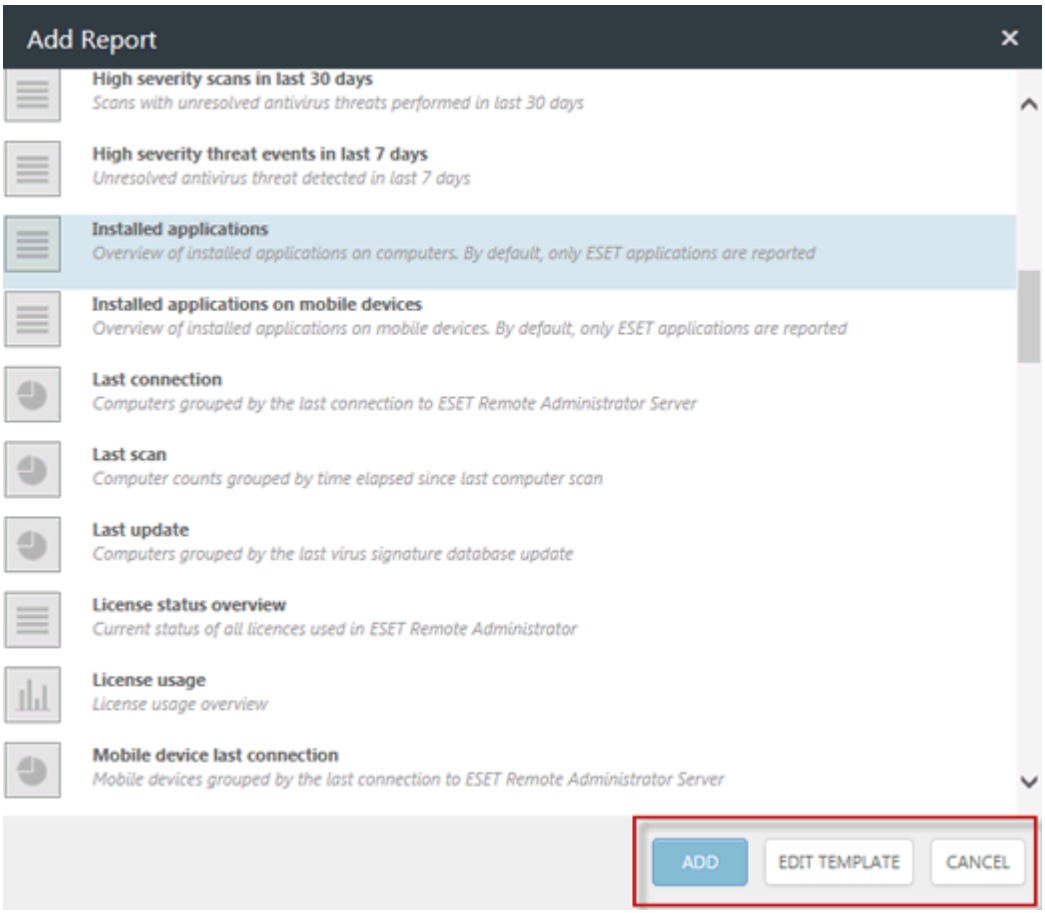




5.1.3 Edit report template

This section details editing existing report templates (for information on how to create a new report template click here).

Click a **blank square** shown in the new dashboard. The **Add Report** window will be displayed. Select **Installed applications** and click **Add** or **Edit Template**.

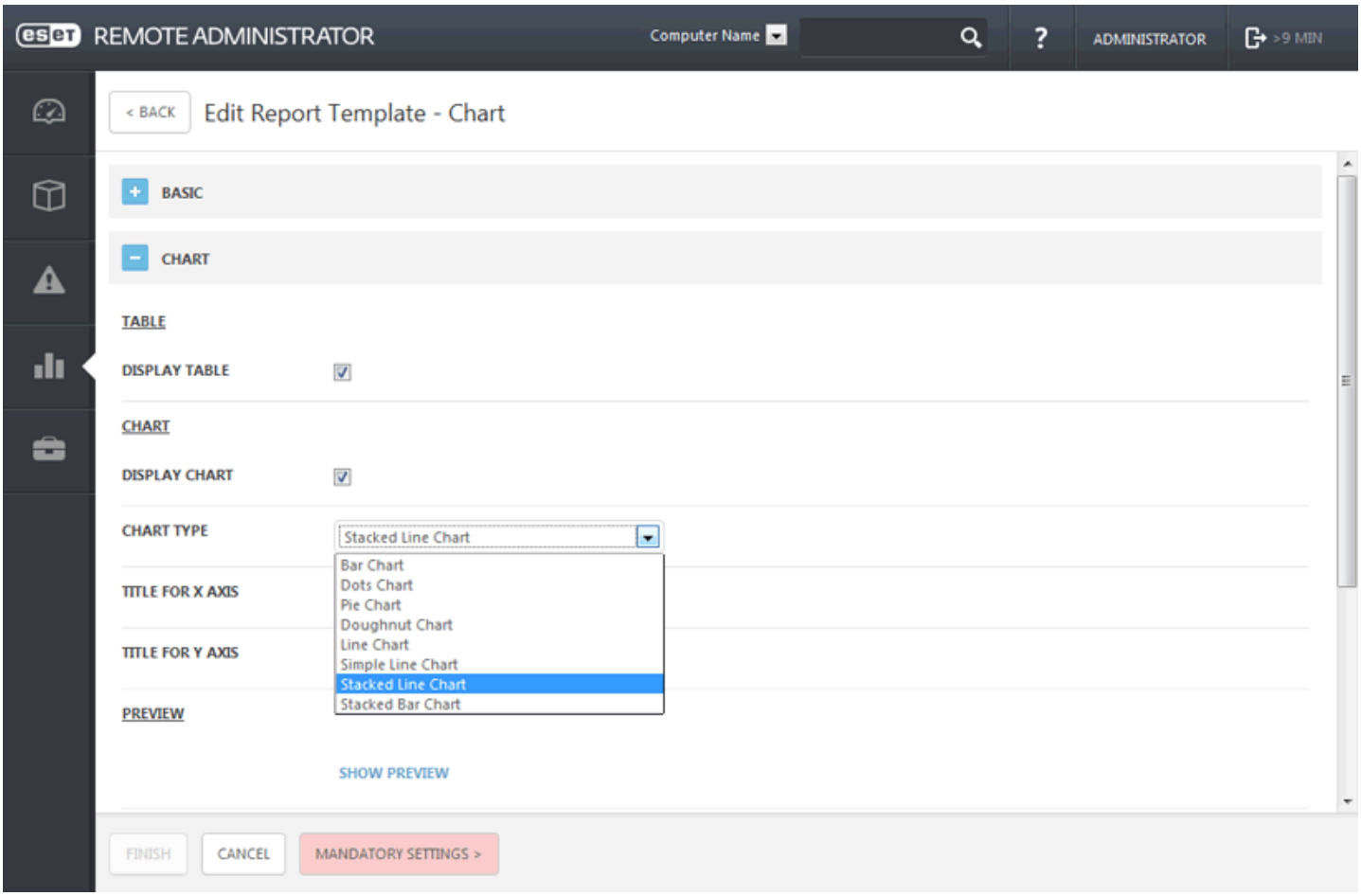

Add Report
High severity scans in last 30 days
Scans with unresolved antivirus threats performed in last 30 days
High severity threat events in last 7 days
Unresolved antivirus threat detected in last 7 days
Installed applications
Overview of installed applications on computers. By default, only ESET applications are reported
Installed applications on mobile devices
Overview of installed applications on mobile devices. By default, only ESET applications are reported
Last connection
Computers grouped by the last connection to ESET Remote Administrator Server
Last scan
Computer counts grouped by time elapsed since last computer scan
Last update
Computers grouped by the last virus signature database update
License status overview
Current status of all licences used in ESET Remote Administrator
License usage
License usage overview
Mobile device last connection
Mobile devices grouped by the last connection to ESET Remote Administrator Server
ADD
EDIT TEMPLATE
CANCEL

Basic

Edit the **Basic** information about the Template. Review or change the **Name**, **Description** and a **Category**. This information is pre-defined according to the selected **Report** type.

Chart

In the **Chart** section, select the **Report** type. In this example, we leave the **Display Table** option empty and select the **Display Chart** option.

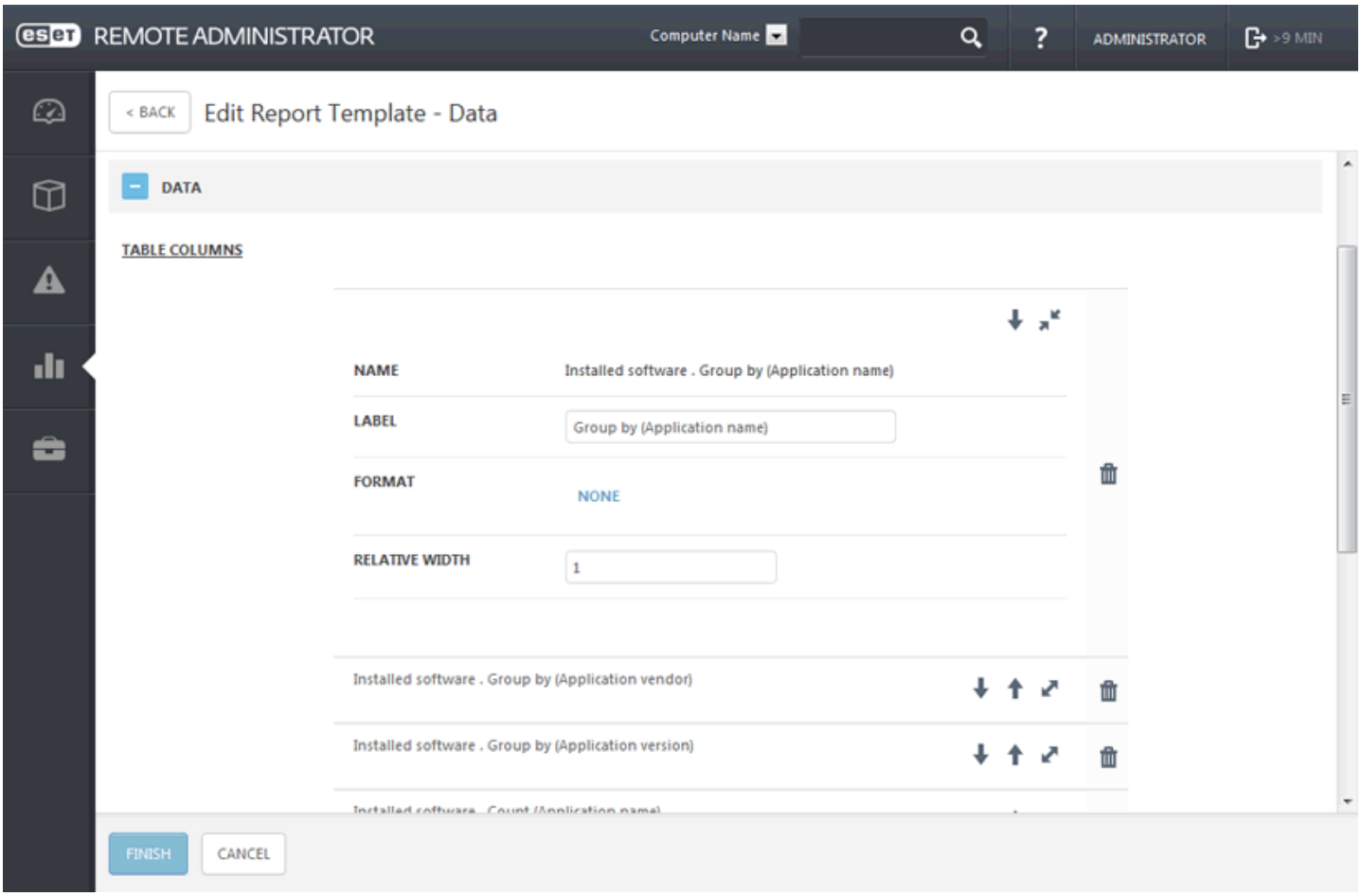


NOTE: Every selected chart type will be displayed in the **Preview** section. This way, you can see what the report will look like in real-time.

Selecting a **Chart** gives you multiple options. For a better overview, we select the **Stacked Line Chart type**. This chart type is used when you want to analyze data with different units of measure.

Optionally, you can define a title for the **X** and **Y** axis of the chart to make reading the chart and identifying trends easier.

Data

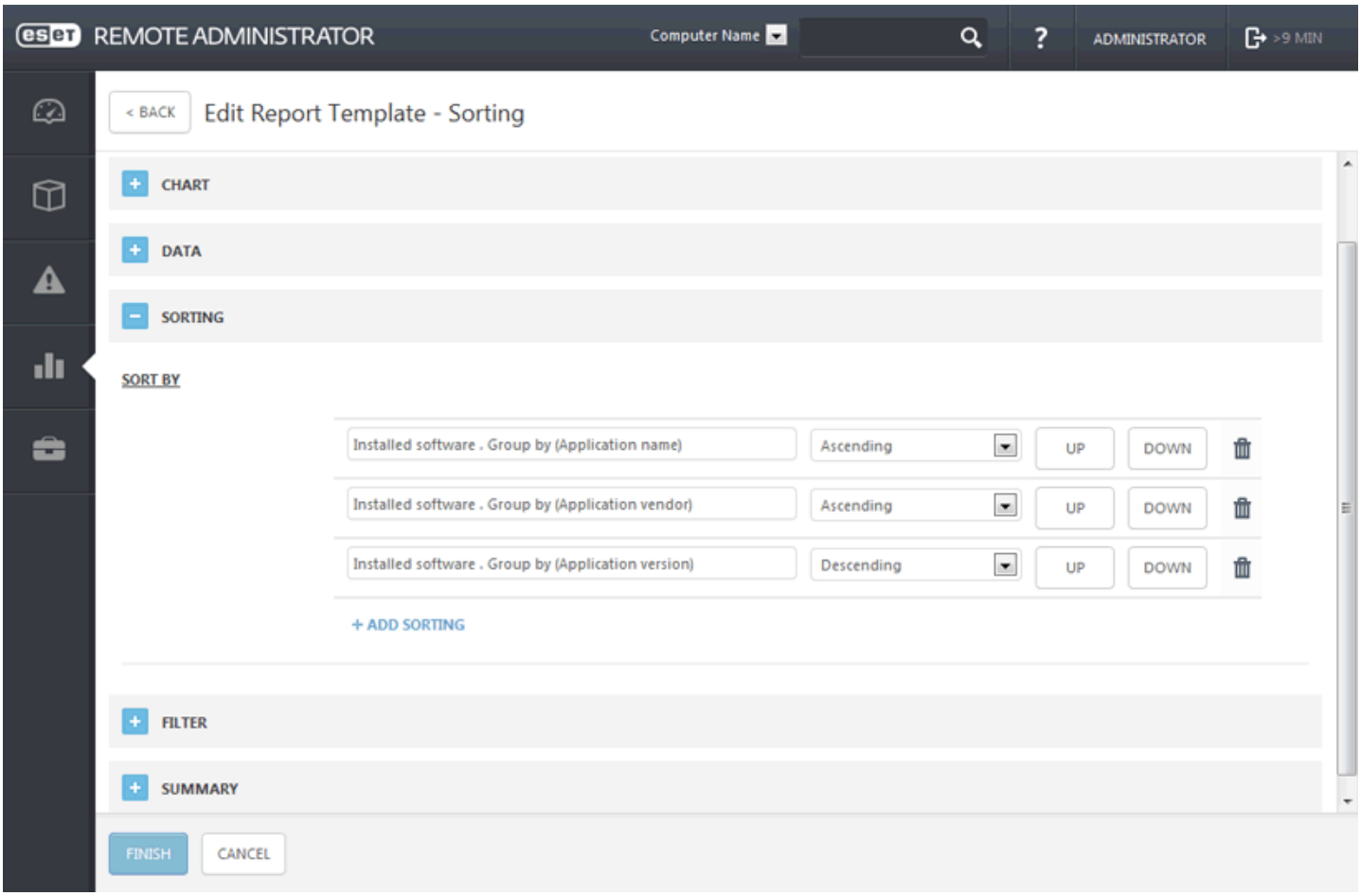


In the **Data** section, we enter the information to be displayed on the **X** and **Y** axis of the chart. Clicking the respective symbols opens a window with options. The choices available for the **Y** axis always depend on the information selected for the **X** axis and vice versa, because the chart displays their relation and the data must be compatible.

For the **X** axis, we select **Computer** > **Computer name** to determine what computers are sending spam. The **Format** will be set to **Value** > **Absolute**. Color and Icons are set by the administrator.

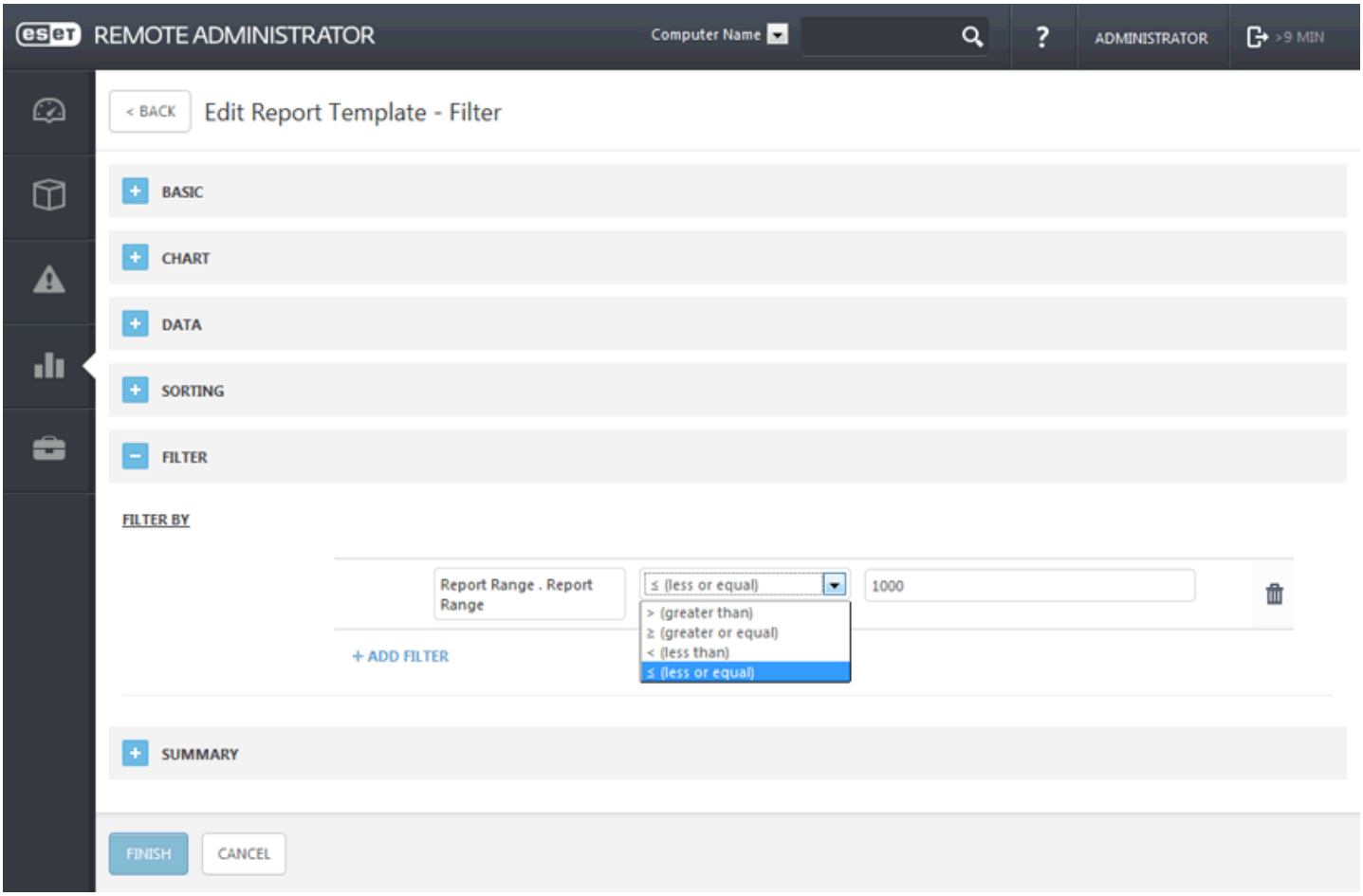
For the **Y** axis, we select **Installed software** > **Size in MB** to determine the absolute number of the spam messages. The **Format** will be set to **Value** > **Absolute**. Color and Icons are set by the administrator.

Sorting



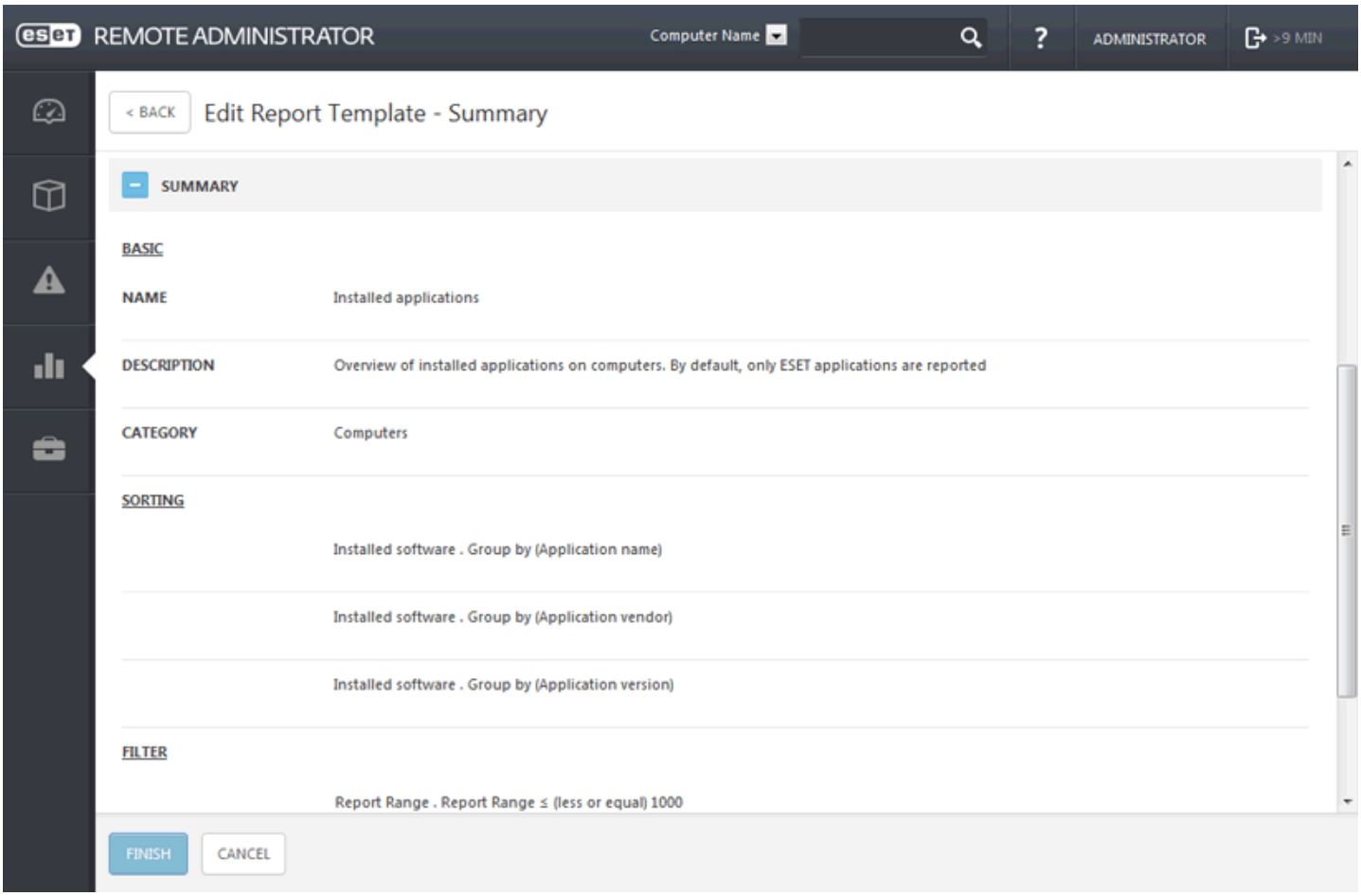
Add sorting to define the relation between the selected data. Select the starting information and then the method, either **Ascending** or **Descending**. It is also possible to sort the data by both options (shown above).

Filter



Options displayed here depend on the settings configured earlier (information for the X and Y axis). Select an option and a mathematical function to determine how the data will be filtered. For this example, we selected **Installed Software** and **Application name** > **is equal to** > **ESS** and **Installed Software**. **Size in MB** > **is greater than** > **50**.

Summary



In the **Summary**, review the selected options and information. If they are to your satisfaction, click **Finish** to create a **Report template**.

5.2 Computers

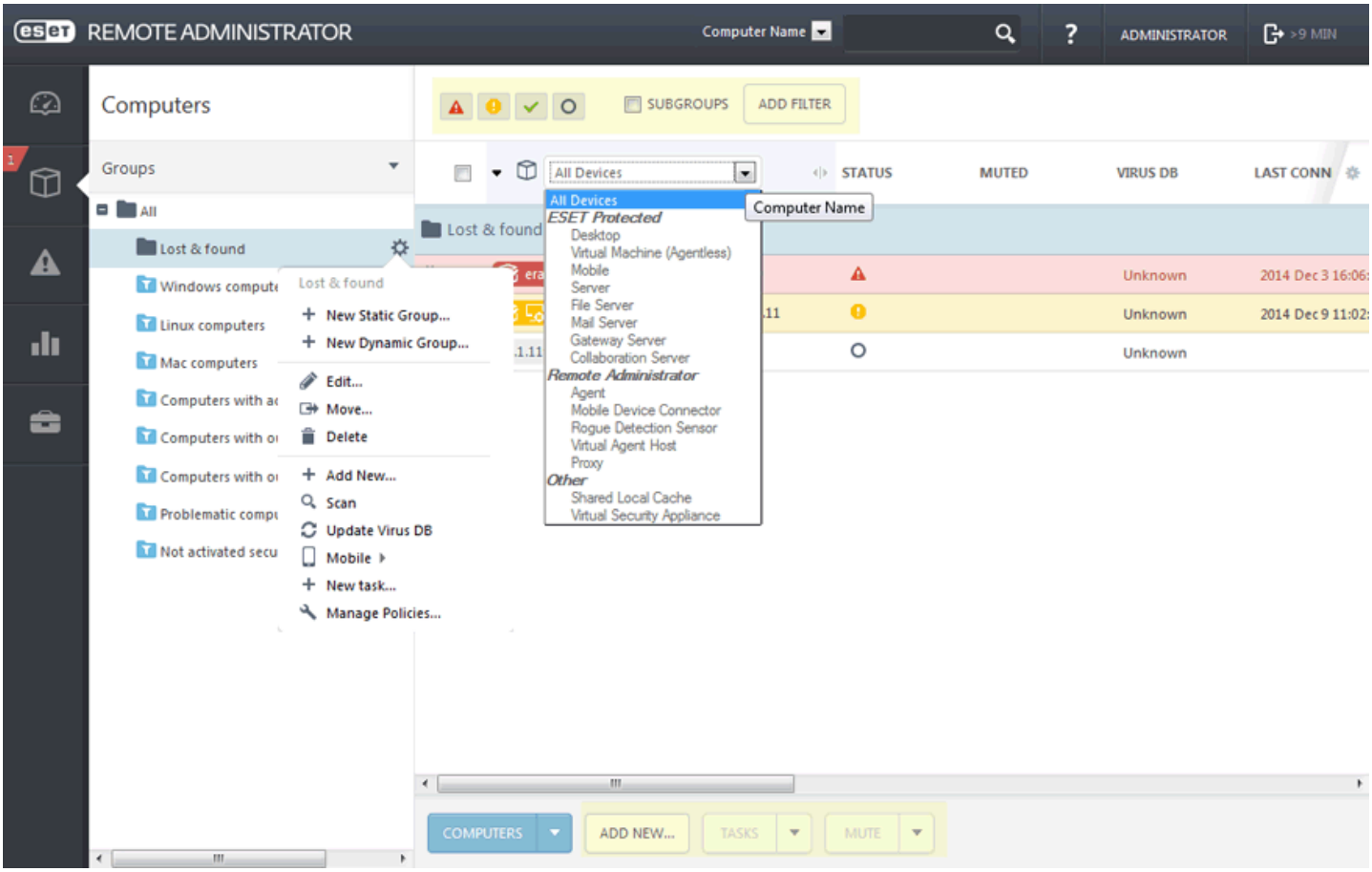
All client computers that were added to ESET Remote Administrator are shown here and are divided into Groups. Clicking on a group from the list (on the left) will display the members (clients) of this group in the right pane. You can filter the clients using the filters at the top of the page, clicking **Add Filter** shows the available filtering criteria. There are also a few pre-defined filters that are quickly accessible:

- Four icons that let you filter by severity (red - **Errors**, yellow - **Warnings**, green - **Notices** and gray - **Unmanaged** computers). The severity icon represents the current status of your ESET product on a particular client computer. You can use a combination of these icons by turning them on or off. For example, to see only the computers with warnings, leave only the yellow icon on (the rest if the icons must be turned off). To see both warnings and errors, leave only these two icons on.
- **Subgroups** check box - show subgroups of the currently selected group.
- **Unmanaged** computers (clients on the network that do not have the ERA Agent or a ESET security product installed) usually appear in the **Lost & Found** group.

Using the drop-down menu below the filters, you can limit the displayed clients (computers). There are a few categories:

- **All Devices** from the drop-down menu to see all the client computers again, without limiting (filtering) displayed clients. You can use a combination of all the above filtering options when narrowing down the view.
- **ESET Protected** (protected by an ESET product)
- **Remote Administrator** (individual ERA components such as Agent, RD Sensor, Proxy, etc.)
- **Other** (Shared Local Cache, Virtual Appliance). When you make your selection, only the respective clients will be displayed.

NOTE: If case you are not able to find a particular computer in the list and know it is in your ERA infrastructure, make sure that all filters are turned off.



You can use context menu (cogwheel ⚙ icon) to can create Static or Dynamic Group, create New task or select from other available actions.

Computers button actions:

+ New...
Manually Add Devices that are not found or added automatically.

Details...
- **Basic** (Name, Parent Group, Device, OS Information, etc.)
- **Configuration** (Configuration, Applied Policies, etc.)
- **Task Executions** (Occurred, Task Name, Task Type, Status, etc.)
- **Installed Applications** (Name, Vendor,Version, Agent supports uninstall, etc.)
- **Alerts** (Problem, Status, etc.)
- **Threats** (All Threat Types, Muted, Cause, etc.)
- **Quarantine** (Threat Name, Threat Type, Object Name, Hash, etc.)

Delete
This will remove the client from the list, but as long as it is in the network it will appear in the **Lost & Found** group.

Move...
You can move the client to a different group, selecting this option displays a list of available groups.

Manage Policies...
A Policy can also be assigned directly to a client (multiple clients), not just a group. Select this option to assign the policy to selected client(s).

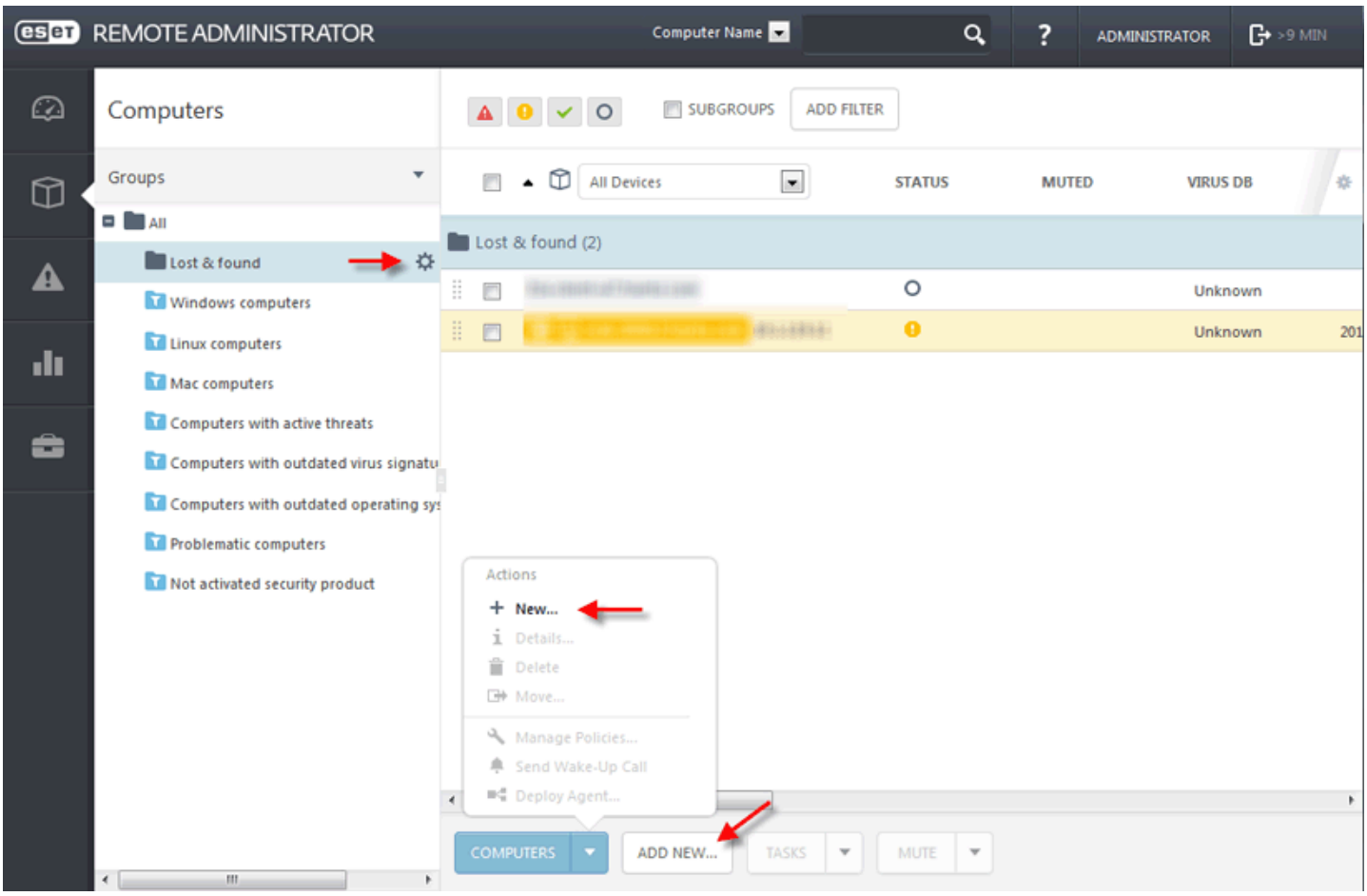
Send Wake-Up Call
ERA Server initiates immediate communication with the ERA Agent on a client machine. This useful when you do not want to wait for the regular interval when the ERA Agent connects to the ERA Server. For example when you want a Client Task to be run immediately on client(s) or if you want a Policy to be applied right away.

NOTE: When you make a change and want it to be applied, wait about one minute before using Wake-Up Call.

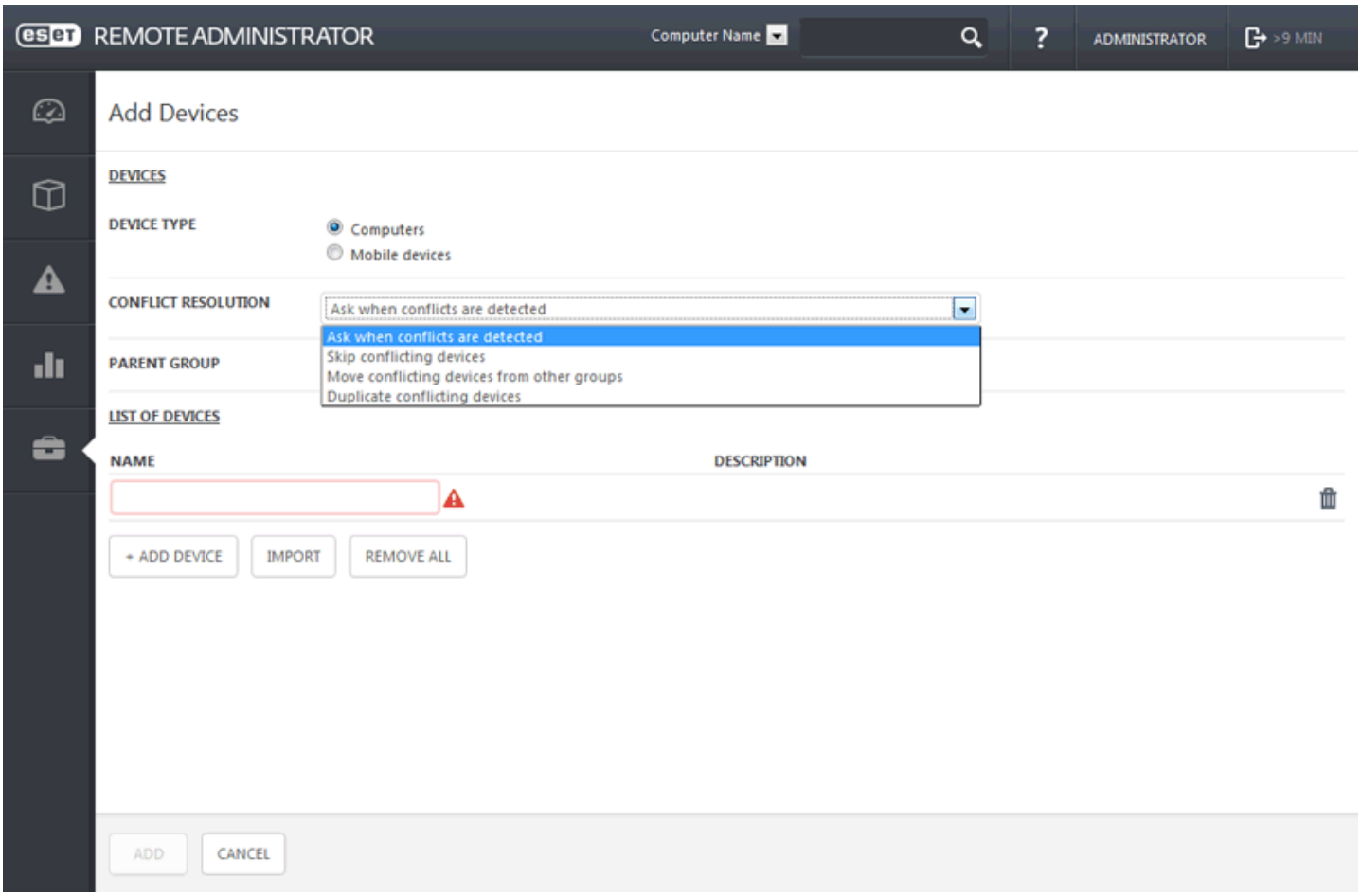
Deploy Agent...
With this option, you can create a New Server Task.

5.2.1 Add Computers

From the **Computers** tab there are three ways to add new computers. For example, select a Static Group, click the cogwheel icon and select + **Add New**.



Type the name of the computer you want to add into the **Name** field. Click + **Add Device** to add additional computers or click Import to import a file with a list of computers to add. Optionally, you can enter a **description** of the computers.



Use the **Conflict Resolution** drop-down menu to select the action to take if a computer you are adding already exists in ERA:

Ask when conflicts are detected: When a conflict is detected, the program will ask you to select an action (see the options below).
Skip conflicting computers: Duplicate computers will not be added.
Move conflicting computers from other groups: Conflicting computers will be moved from their original groups to the **All** group.
Duplicate conflicting computers: New computers will be added, but with different names.

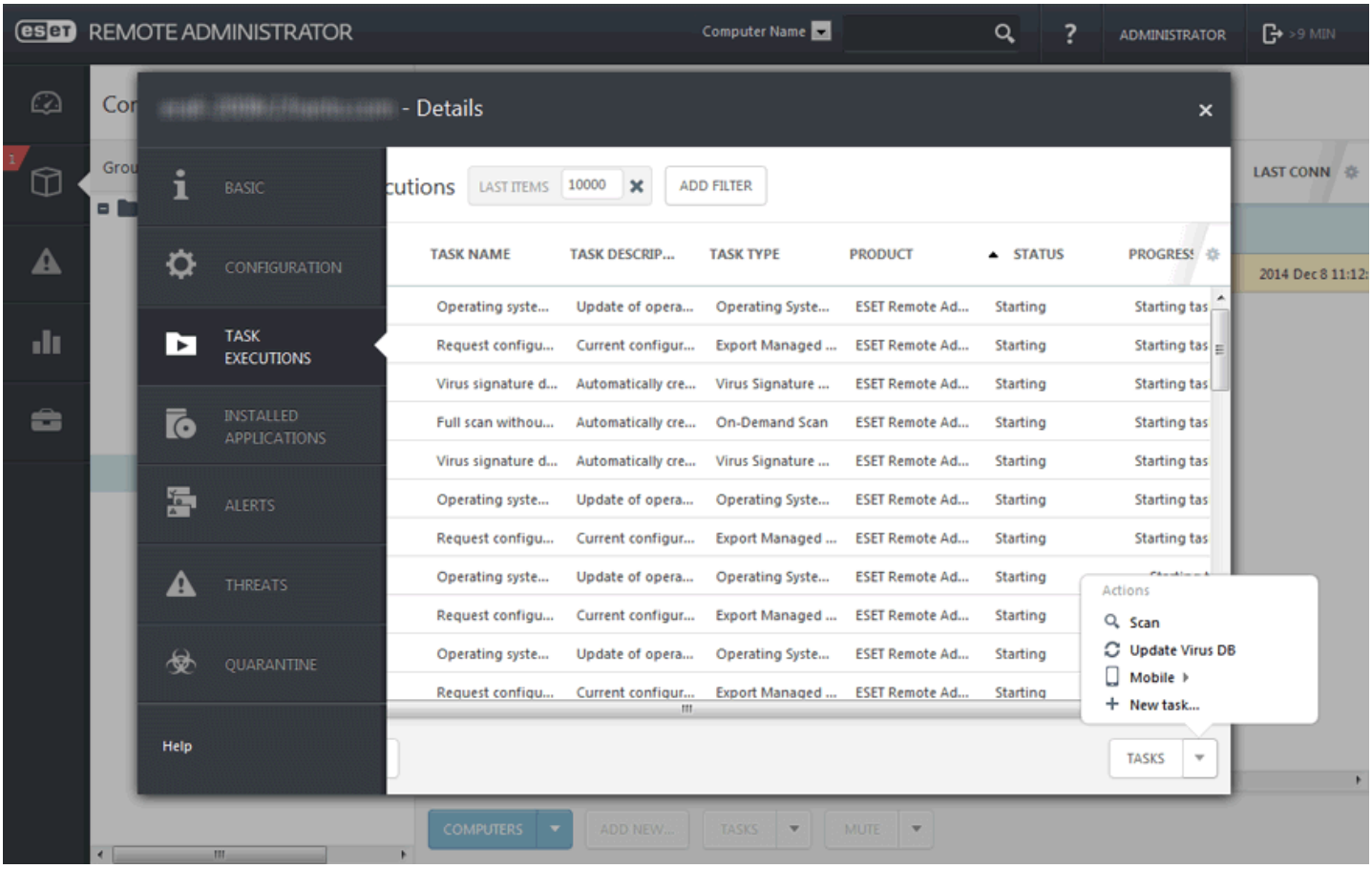
Click **Add**. Computers can be viewed in the list on the right when you select the group they belong to.

NOTE: Adding multiple computers may take a longer time, reverse DNS lookup may be preformed.

For more information how to add Mobile devices see chapter Mobile device enrollment.

5.2.2 Computer details

Select a computer in Static or Dynamic Group and click **Details** to view more information about that computer.



The Computer details menu contains the following settings:

- **Basic** - you can change the computer's Name, description and parental group.
- **Configuration -** displays the entire configuration, connection and applied policies for this computer.
- **Task Executions -** Occurred, Task Name, Task Type, Status
- **Installed Applications -** Name, Version, Size, Agent supports uninstall
- **Alerts** - Problem, Status, etc.
- **Threats -** All Threat Types, Muted, Cause etc.
- **Quarantine -** Threat Name, Type, Object Name, Hash etc.

Tasks button actions

After selecting a computer or set of computers and clicking **Tasks**, the following options will be available:

Scan

Using this option will run the On Demand Scan task on the client that reported the threat.

Update Virus DB

Using this option will run the Virus Signature Database Update task (triggers an update manually).

Mobile

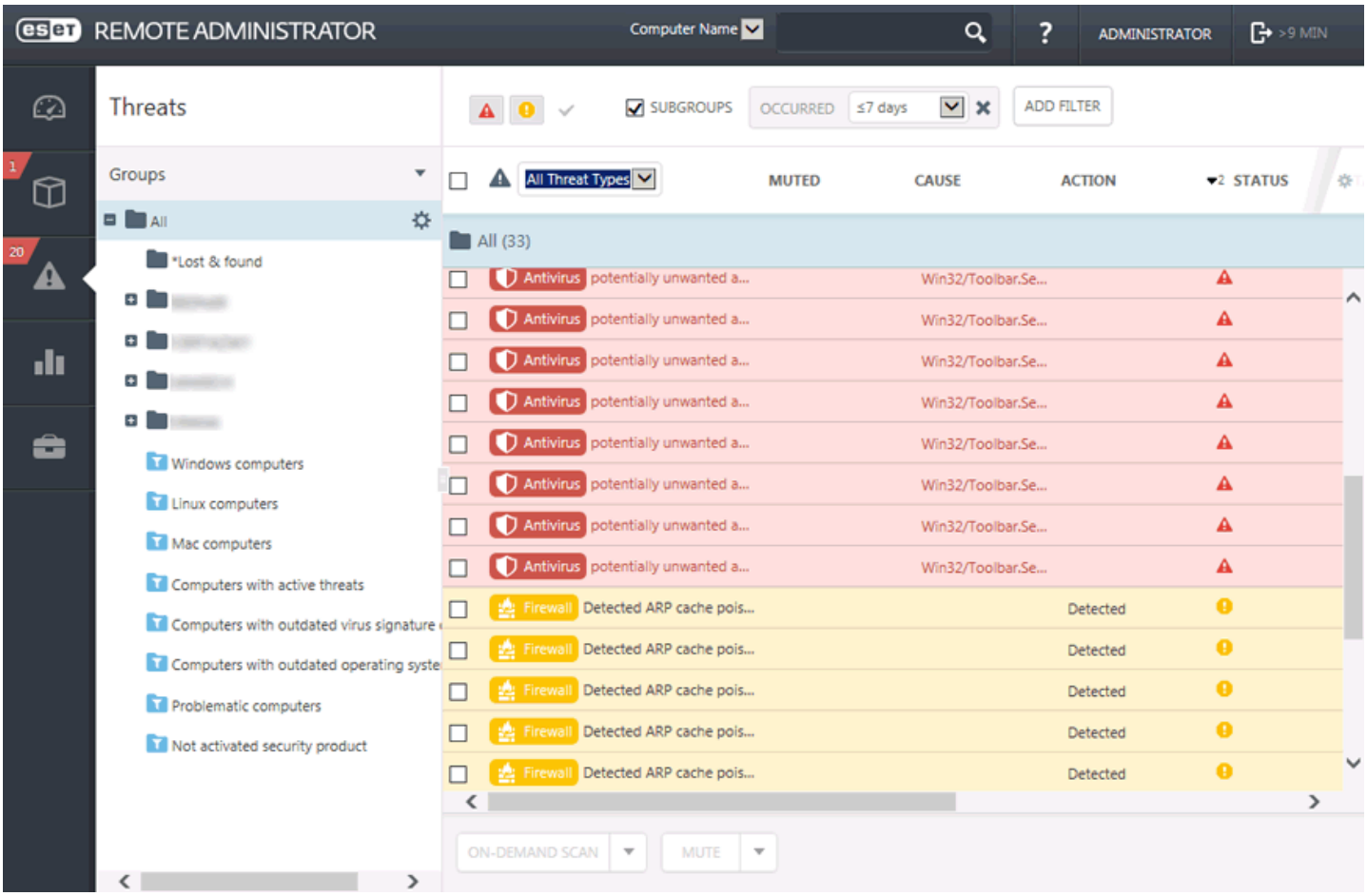
- **Enroll...** - with this option, you can create a new client task.
- **Find** - if you want to request the GPS coordinates of your mobile device.
- **Lock** - device will be locked when suspicious activity is detected or the device is marked as missing.
- **Unlock** - device will be unlocked.
- **Siren** - triggers a loud siren remotely, the siren will start even if your device is set to mute.
- **Wipe** - all data stored in your device will be permanently erased.

+ New task...
Select a task and configure throttling (optional) for this task. The task will be queued according to the task settings. This option immediately triggers an existing task, that you select from a list of available tasks. The trigger is not available for this task, because it will be executed immediately.

Mute
If you select a computer and press **Mute**, the Agent of this client stops reporting to ERA, it will only aggregate the information. A mute icon will be displayed next to a computer name in the Muted column.
Once muting is disabled by clicking **Mute** > **Un-mute**, the muted computer will report again and communication between ERA and the client is restored.

5.3 Threats

The **Threats** section gives you an overview of all threats found on computers in your network. On the left side, the Group structure is displayed. Here you can browse groups and view threats on members of a given group. Select group **All** and use filter **All threats types** to display all threats found on clients in all groups.



Filtering threats

You can filter threats using a filter above the list. By default, all threat types from the last 7 days are shown. To add multiple filtering criteria, click **Add filter** and select an item from the list - you can filter the results by **Name** (name of the threat), **Cause** (cause of the threat) or the **IPv4/IPv6** address of the client that reported this **Threat**.

By default, all threat types are displayed, but you can filter by **Anti-virus** and **Firewall** threats for a more specific view.

On-demand scan

Using this option will run the On Demand Scan task on the client that reported the threat.

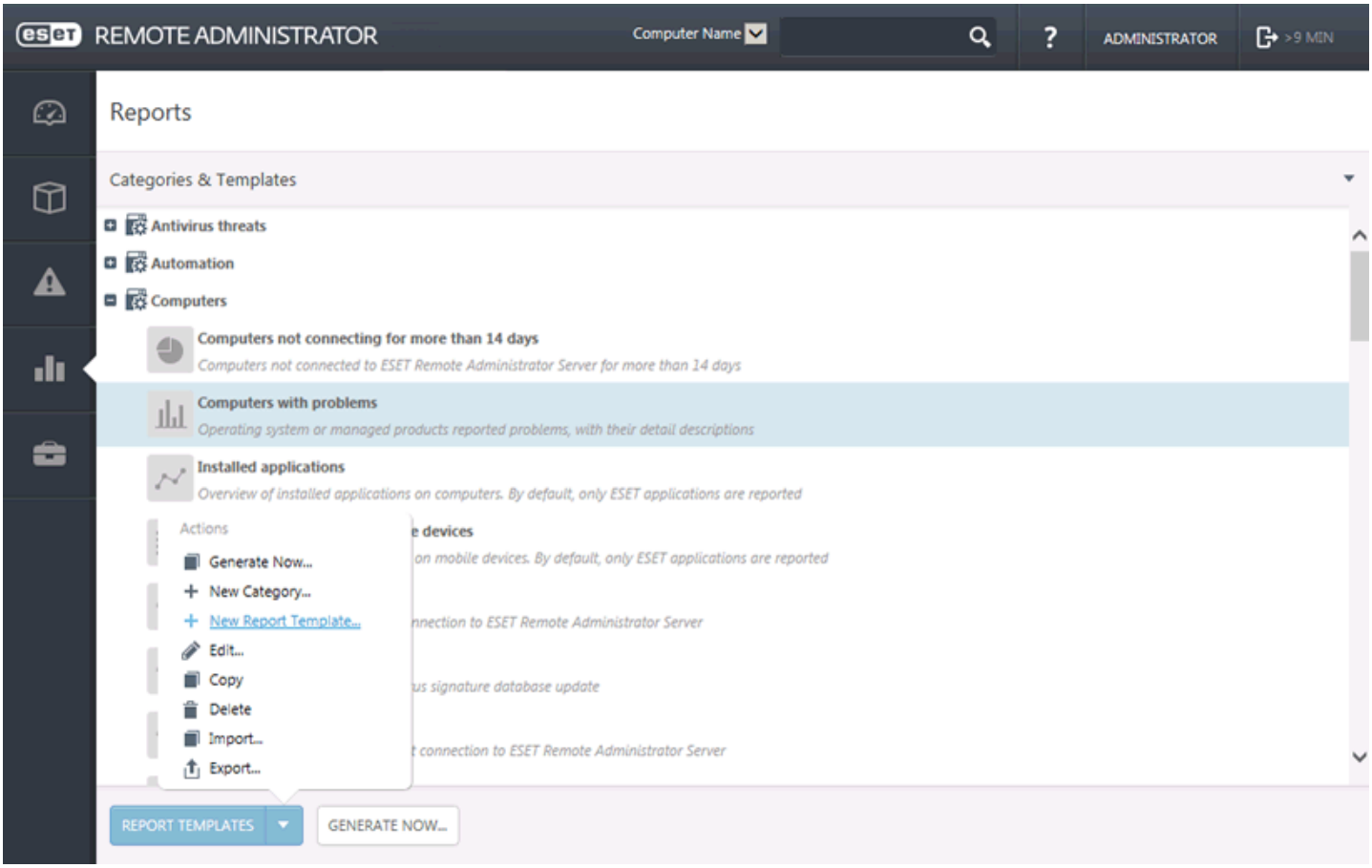
Mute

Selecting mute on a specific threat mutes this threat (not the client). This report will no longer be displayed as active. You can also choose to mute the client (select **Mute** from the context menu on the threat) that reported this threat.

5.4 Reports

Reports allow you to access and filter data from the database in a convenient way. Reports are divided into categories for a better overview, each category includes a short description about the report itself. Click **Generate Now** at the bottom of the page to create a report based on a selected template and then display this report.

You can use predefined report templates from the list of **Categories & Templates**, or you can create a new report template with custom settings. Click Create a new report template to view settings for each report in detail and specify custom settings for a new report.



Selecting a report will bring up the **Actions** context menu, which appears after clicking **Report templates** at the bottom of the page. The following options are available:

Generate now... - select a report from the list and navigate to **Report templates** > **Generate Now...**, or simply click **Generate now...**. The report will be generated and you can review the output data.

New Category... - enter a **Name** and a **Description** to create a new category of report templates.

New report template... - create a new custom report template.

Edit... - edit an existing report template. The same settings and options apply as for creating a new report template (see above).

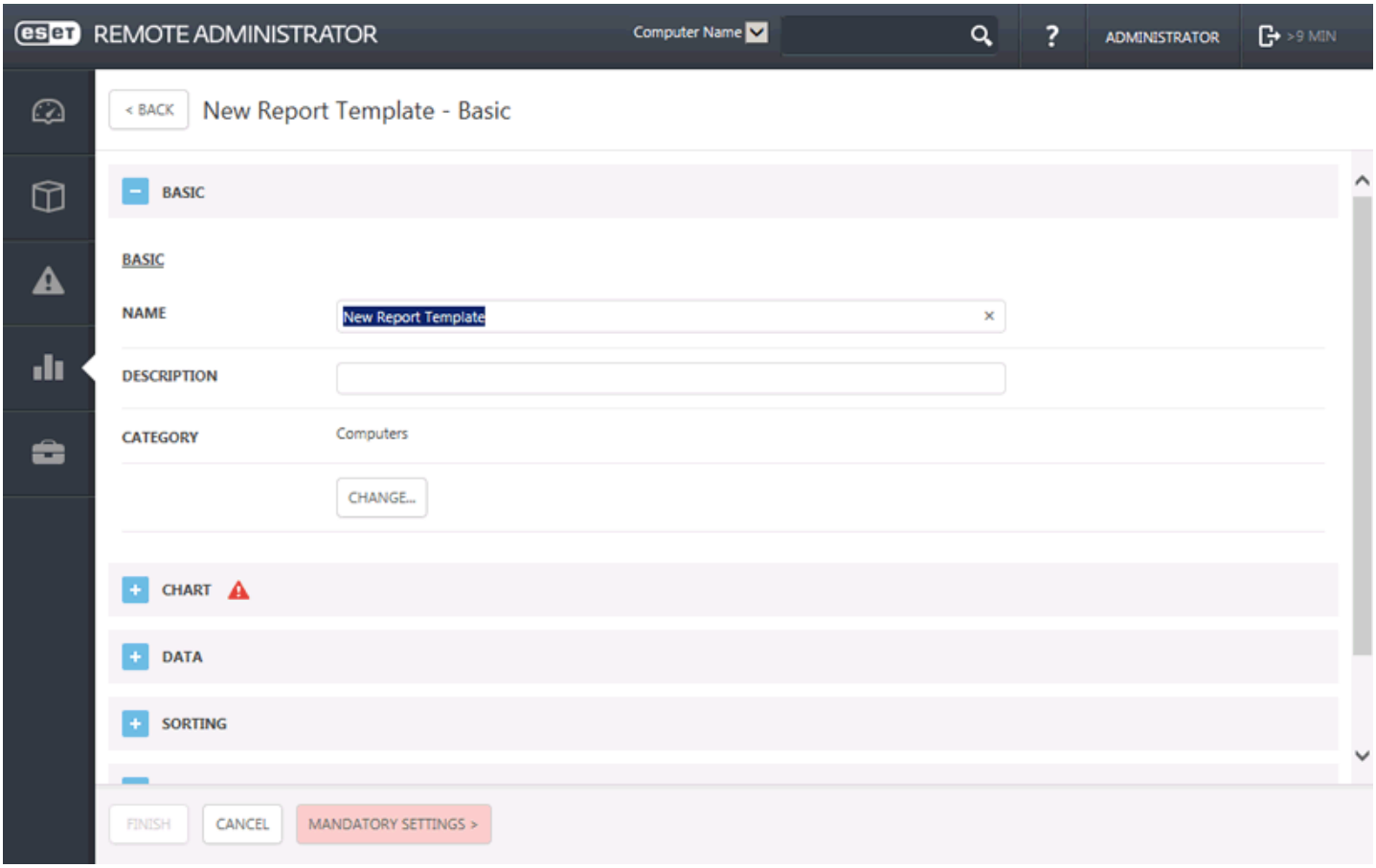
Copy - only use **Copy** if you want to make small adjustments to an existing report template. **Copy** an existing report template and then **Edit** the settings to create a new template.

Delete - remove the selected report template completely.

Import/ Export - Select a report from the list and navigate to **Report templates** > **Export...**. The report (with the data defined in the report) will be generated and saved to a *.txt* file.

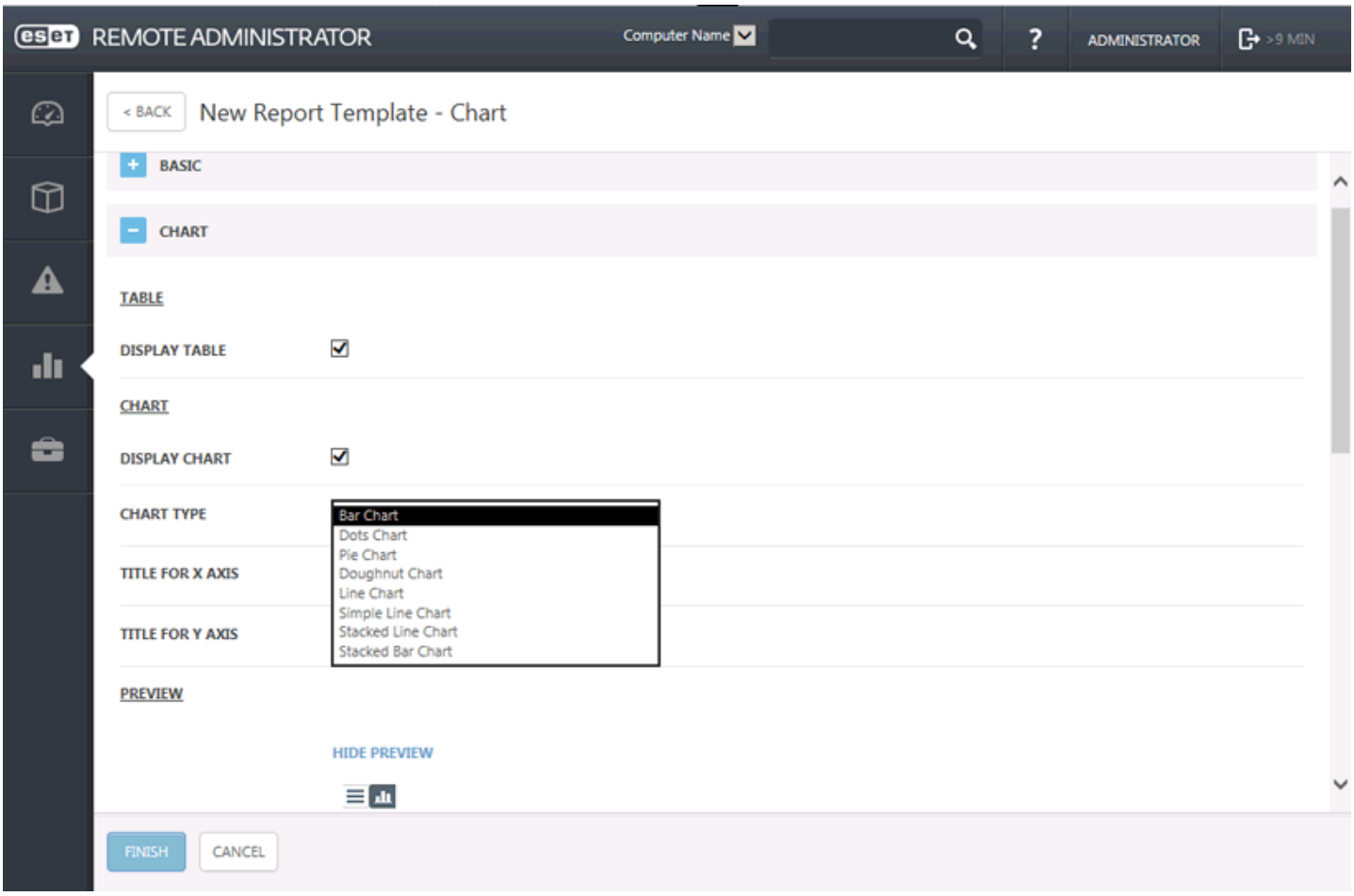
5.4.1 Create a new report template

Navigate to **Reports** and click **Report templates** under **Categories & Templates** on the left. From the pop up window, select **New Report Template...**.



Basic

Edit the Basic information about the Template. Enter a **Name**, **Description** and **Category**. This can be either a pre-defined Category, or you can create a new one (use the **New Category** option described in the previous chapter).



Chart

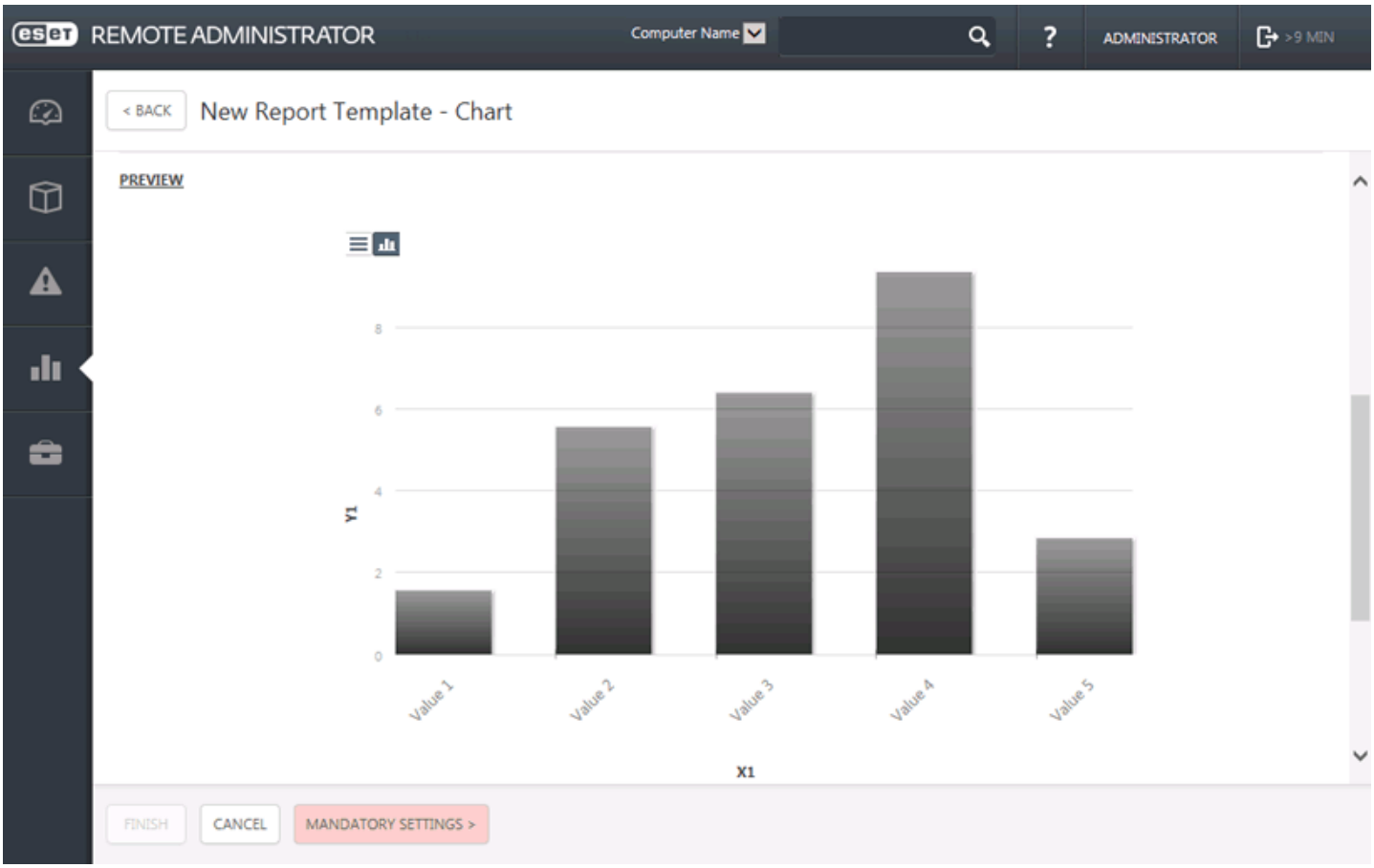
In the **Chart** section, select the **Report** type. Either a **Table**, where the information is sorted in rows and columns, or a **Chart**, that represents data using an X and Y axis.

NOTE: The selected chart type will be displayed in the **Preview** section. This way, you can see what the report will look like in real-time.

Selecting a **Chart** gives you multiple options:

- **Bar chart** - A chart with rectangular bars proportional to the values they represent.
- **Dots bar chart** - In this chart, dots are used to display quantitative values (similar to a bar chart).
- **Pie chart** - A pie chart is a circular chart divided into proportional sectors, representing values.
- **Doughnut chart** - Similar to a pie chart, but the doughnut chart can contain multiple types of data.
- **Line chart** - Displays information as a series of data points connected by straight line segments.
- **Simple line chart** - Displays information as a line based on values without visible data points.
- **Stacked line chart** - This chart type is used when you want to analyze data with different units of measure.
- **Stacked bar chart** - Similar to a simple bar chart, but there are multiple data types with different units of measure stacked in the bars.

Optionally, you can enter a title for the **X** and **Y** axis of the chart to make it easier to read the chart and recognize trends.



Data

In the **Data** section, select the information you want to display:

a. **Table Columns**: Information for the table is added automatically based on the selected report type. You can customize the **Name**, **Label** and **Format** (see below).

b. **Chart Axes**: Select the data for the **X** and the **Y** axis. Clicking the respective symbols opens a window with options. The choices available for the **Y** axis always depend on the information selected for the **X** axis and vice versa, because the chart displays their relation and the data must be compatible. Select the desired information and click **OK**.

You can change the **Format** in which the data is displayed to any of the following:

- **Data Bar** (only for the bar charts) / **Value** / **Color** / **Icons**

Sorting

Add Sorting to define the relation between the selected data. Select the starting information (sorting value) and sorting method, either **Ascending** or **Descending**. This will define the outcome displayed in the chart.

Filter

Next, define the filtering method. Select the filtering value from the list and its value. This defines what information will be displayed in the chart.

Summary

In the **Summary**, review the selected options and information. If they are to your satisfaction, click **Finish** to create a new report template.

Every report in the dashboard has its own options for customization - click the wheel symbol in the upper right corner to view them. Here, you can **Refresh** the displayed information, **Change** to a different report, **Edit** the report template (see options above), set a new **Refresh** interval that defines how often the data in this report is refreshed or **Rename**/**Remove** the report. Using the arrows in the symbol below, you can customize the size of the report. You can make more relevant reports larger, less relevant reports smaller and so on. Click **toggle fullscreen** to view a report in fullscreen mode.

5.4.2 Generate report

There are two ways to create or edit template:

1. Navigate to **Admin** > **Tasks** > **Server Tasks**. Select **New...** to create a new Generate Report task.
2. Select a report template from which you want to generate a report. You can use and edit a pre-defined report template or create a new report template.

- You can either send this report in an e-mail (in a file format defined here) or save it to file directly. Clicking either option displays the corresponding settings below.
- Configure the settings (as described in the Generate Report task) and click **Finish**.
- The task is now created and displayed in the **Task types** list. Select this task and click **Run Now** on the bottom of the page. The task will be executed immediately.

5.4.3 Schedule a report

1. Navigate to **Admin** > **Tasks** > **Server Tasks**. Select **New** to create a new **Generate Report** task.
2. Select a report template from which you want to generate a report. You can use and edit a pre-defined report template, or create a new report template.

- You can either send this report in an e-mail (in a file format defined here) or save it to a file. Clicking either option displays the corresponding settings below.
- Configure the settings (as described in the Generate Report task). This time, we will create a **Server Trigger** for this task.
- In the **Trigger** section, navigate to **Settings**. Select **Scheduled trigger** and the time when you want this task to run.
- Click **Finish**. The task is created and will run at the period defined here (either one time, or repeatedly).

5.4.4 Outdated applications

To see what which ERA components are not up to date, use report called **Outdated applications**.

There are two ways to do that:

1. Add a New Dashboard, click one of the tiles and a pop-up screen with **Report Templates** listed will be displayed. Select a report **Outdated applications** from the list and click **Add**.
2. Go to **Reports**, navigate to **Computers** category, select **Outdated applications** template from the list and **Generate now...** button at the bottom. The report will be generated and you can review the output data.

To upgrade the components, use Client Task Administrator Components Upgrade.

6. Administration of ESET Remote Administrator

The Administration of ESET Remote Administrator section discusses how to manage and configure ESET Remote Administrator. Read on through the Admin chapter.

6.1 Admin

The **Admin** section is the main configuration component of ESET Remote Administrator. This section contains all the tools that administrator can use to manage client security solutions, as well as the ERA Server settings. You can use Admin tools to configure your network environment in such a way that it won't require a lot of maintenance. Also, you can configure notifications and dashboards which will keep you aware of the status of your network.

In this section

- Dynamic Group Templates
- Groups
- Policies
- Client tasks
- Server tasks
- Triggers
- Notifications
- Peer Certificates
- Access Rights
- Server Settings
- License Management

6.1.1 Groups

Groups allow you to manage and categorize computers. You can then easily apply different settings, tasks or restrictions to client computers based on their presence in a particular group. You can use pre-defined groups and group templates or create new ones.

There are two types of client groups:

Static Groups

Static Groups are groups of select client computers (members). Group members are static and can only be added/ removed manually, not based on dynamic criteria. A computer can only be present in one Static Group.

Dynamic Groups

Dynamic Groups are groups of clients where membership in the group is determined by specific criteria. If a client does not fulfill that criteria, it will be removed from the group. Computers that satisfy the criteria will be added to the group automatically.

The **Groups** window is divided into three sections:

1. A list of all groups and their subgroups is displayed on the left. You can select a group and an action for this group from the context menu (cogwheel next to the group name). The options are the same as described below (Group actions button).
2. Details for the selected group are shown on the right pane (you can switch between tabs):

- **Computers** that are members of the group.
- **Policies** assigned to this group.
- **Tasks** assigned to this group.
- **Summary** basic description of the group.

3. The popover menu buttons **Groups** and **Computers** let you perform all the following actions:

Group actions button

+ New Static Group...
This option becomes available if you click a **Group** in the list on the left. This group will be the default parent group, but you can change the parent group later when you create a new Static Group.

+ New Dynamic Group...
This option becomes available if you click a **Group** in the list on the left. This group will be the default parent group, but you can change the parent group later when you create a new Dynamic Group.

Edit...
Allows you to edit the selected Group. The same settings apply as when you create a new Group (static or dynamic).

Move...
You can select a group and move it as a subgroup of another group.

Delete
Removes the selected group completely.

Import...
You can import a list (usually a text file) of computers, as members of the selected group. If the computers already exist as a members of this group, the conflict will be solved based on the selected action:

- **Skip conflicting computers** (conflicting computers will not be added)
- **Move conflicting computers from other groups** (conflicting computers will be moved here from other groups they belong to
- **Duplicate conflicting computers** (conflicting computers will be added, but with different names).

Export...
Export the members of the group (and subgroups, if selected) in a list (*.txt* file). This list can be used for review, or imported later.

+ Add New...
With this option, you can add a new device.

Scan
Using this option will run the On Demand Scan task on the client that reported the threat.

Update Virus DB
Using this option will run the Virus Signature Database Update task (triggers an update manually).

Mobile

- **Enroll...** with this option, you can create new client task.
- **Find** - if you want to request the GPS coordinates of your mobile device.
- **Lock** - device will be locked when suspicious activity is detected or the device is marked as missing.
- **Unlock** - device will be unlocked.
- **Siren** - triggers a loud siren remotely, the siren will start even if your device is set to mute.
- **Wipe** - all data stored in your device will be permanently erased.

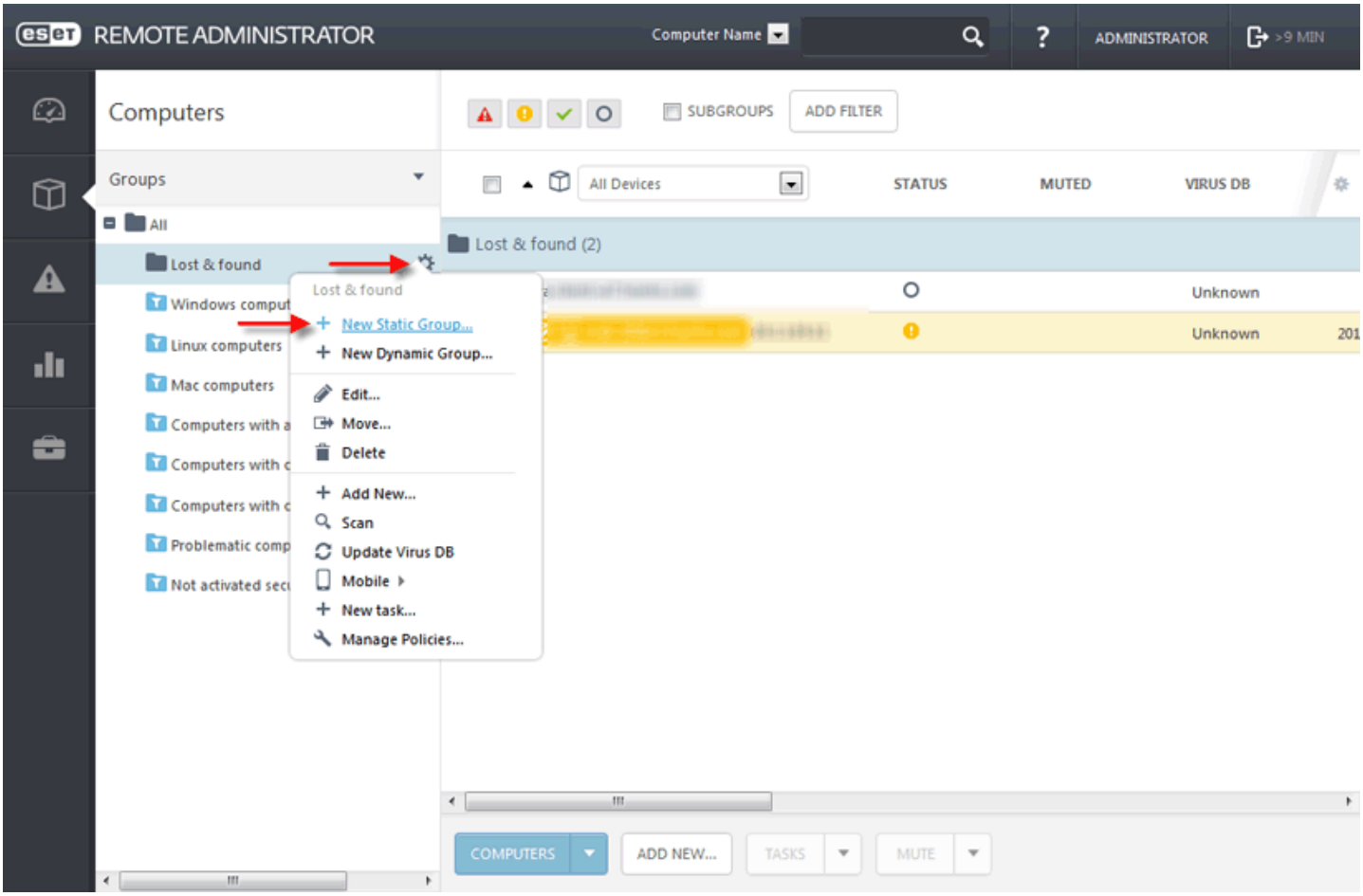
+ New task...
You can create a new Client Task. Select a task and configure the throttling (optional) for this task. The task will be queued according to the task settings.
This option immediately triggers an existing task, that you select from a list of available tasks. The trigger is not available for this task, because it will be executed immediately.

Manage Policies...
Assign a Policy for the selected group.

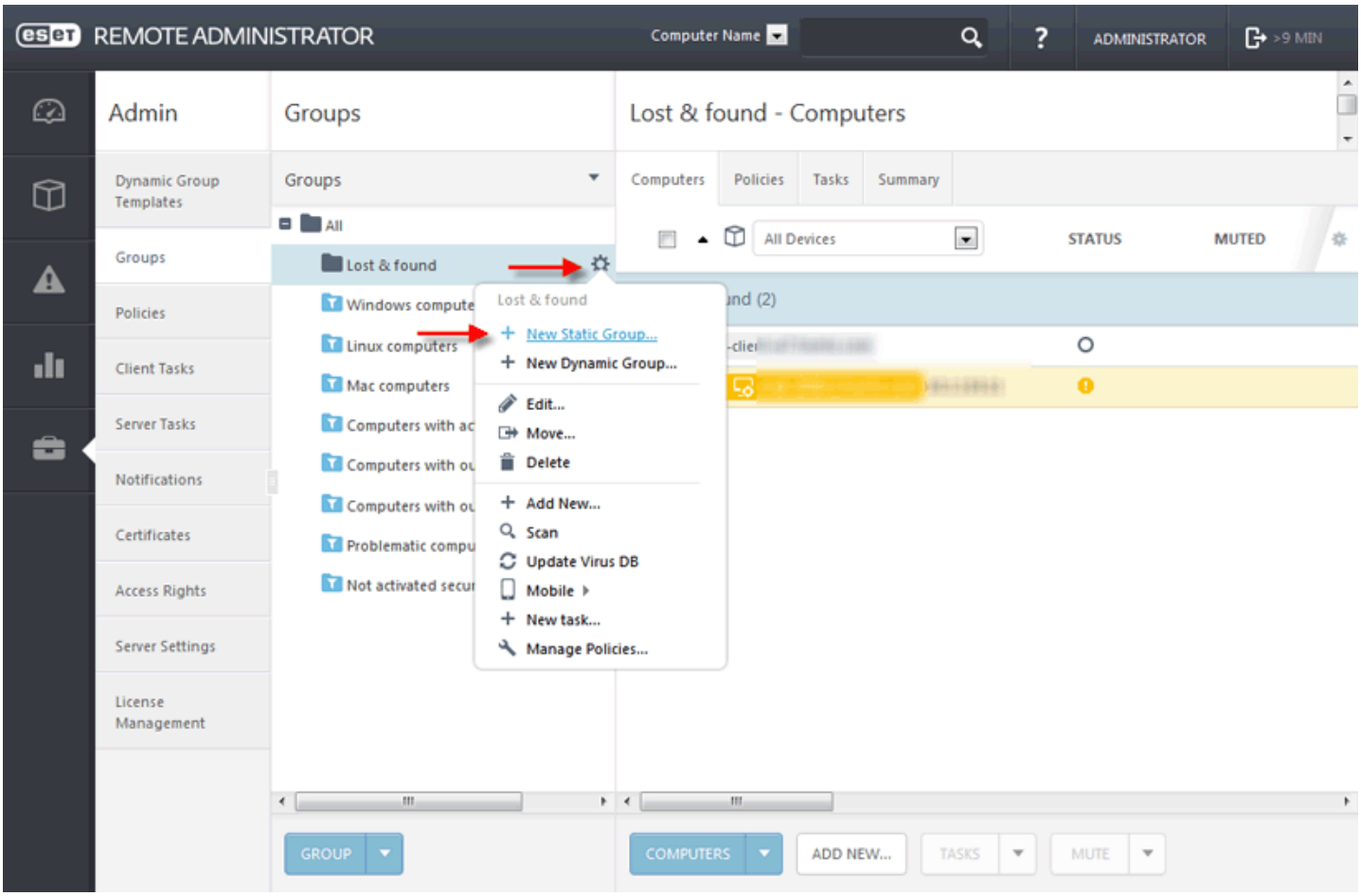
6.1.1.1 Create new Static Group

There are three ways to create a New Static Group:

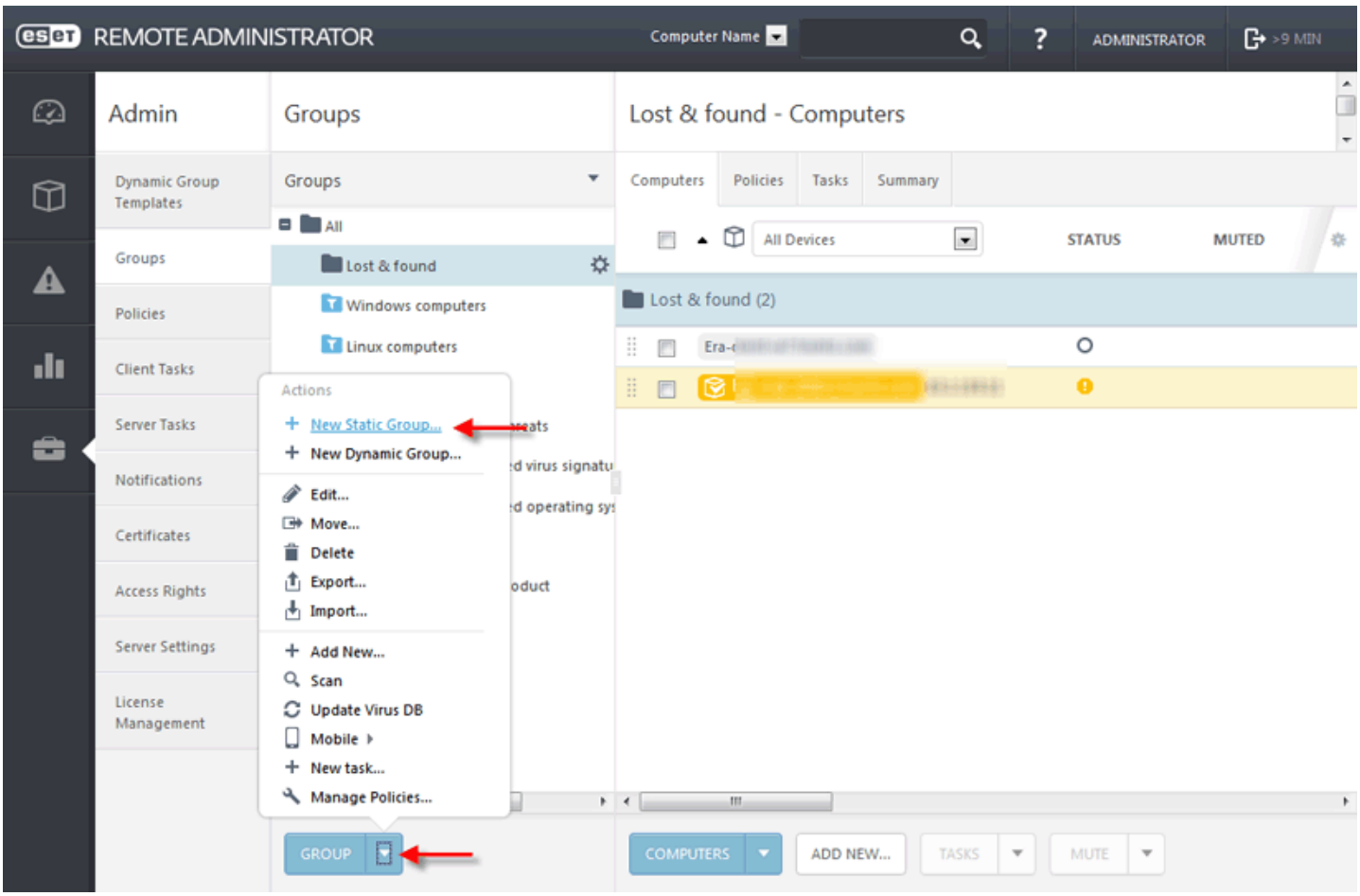
1. Click **Computers** > **Groups** > ⚙ and select **New Static Group...**



2. Click **Admin** > **Groups** > ⚙ > **New Static Group...**

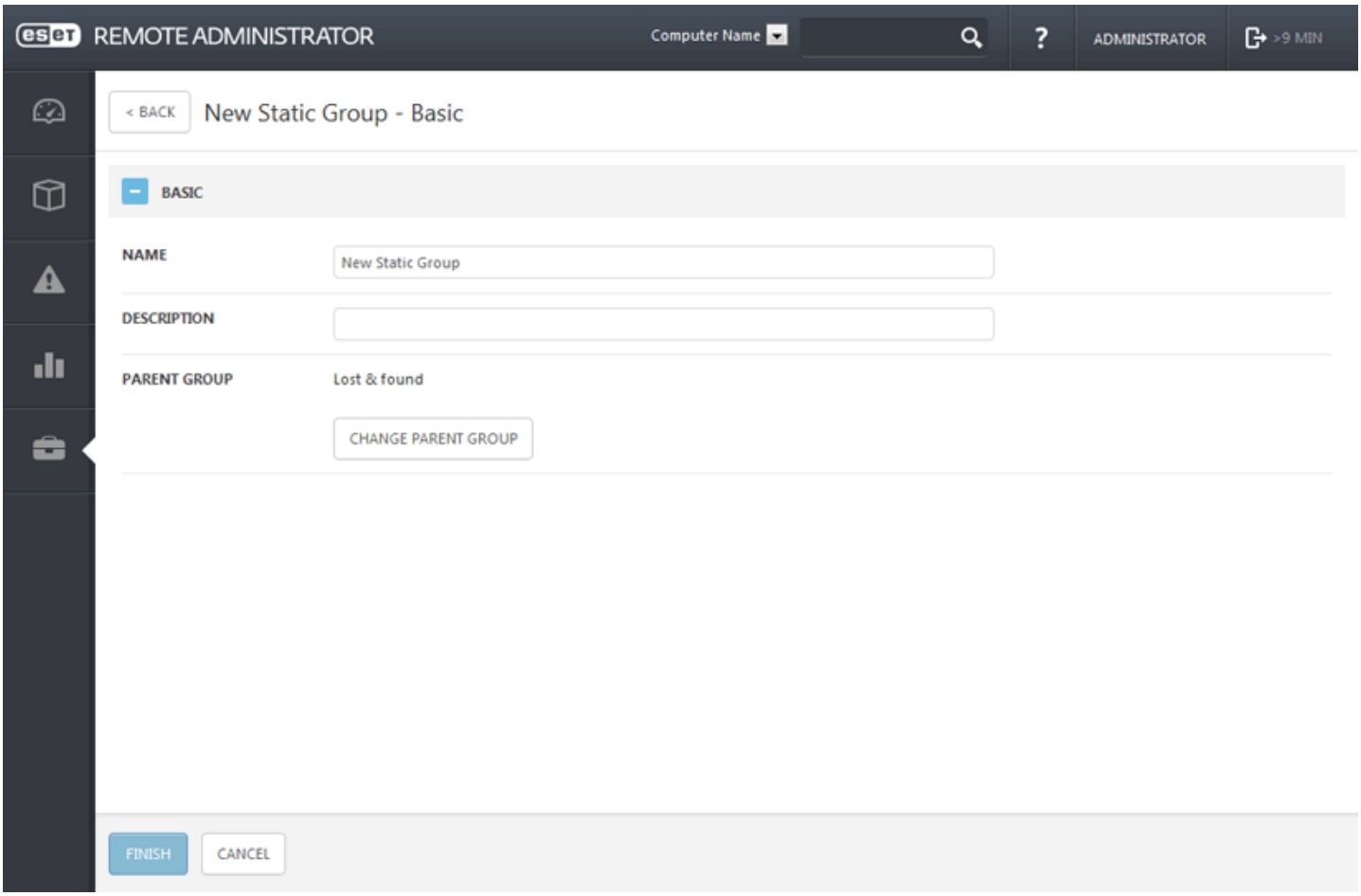


3. Click **Admin** > **Groups** > select a Static Group and click **Group**.



Basic

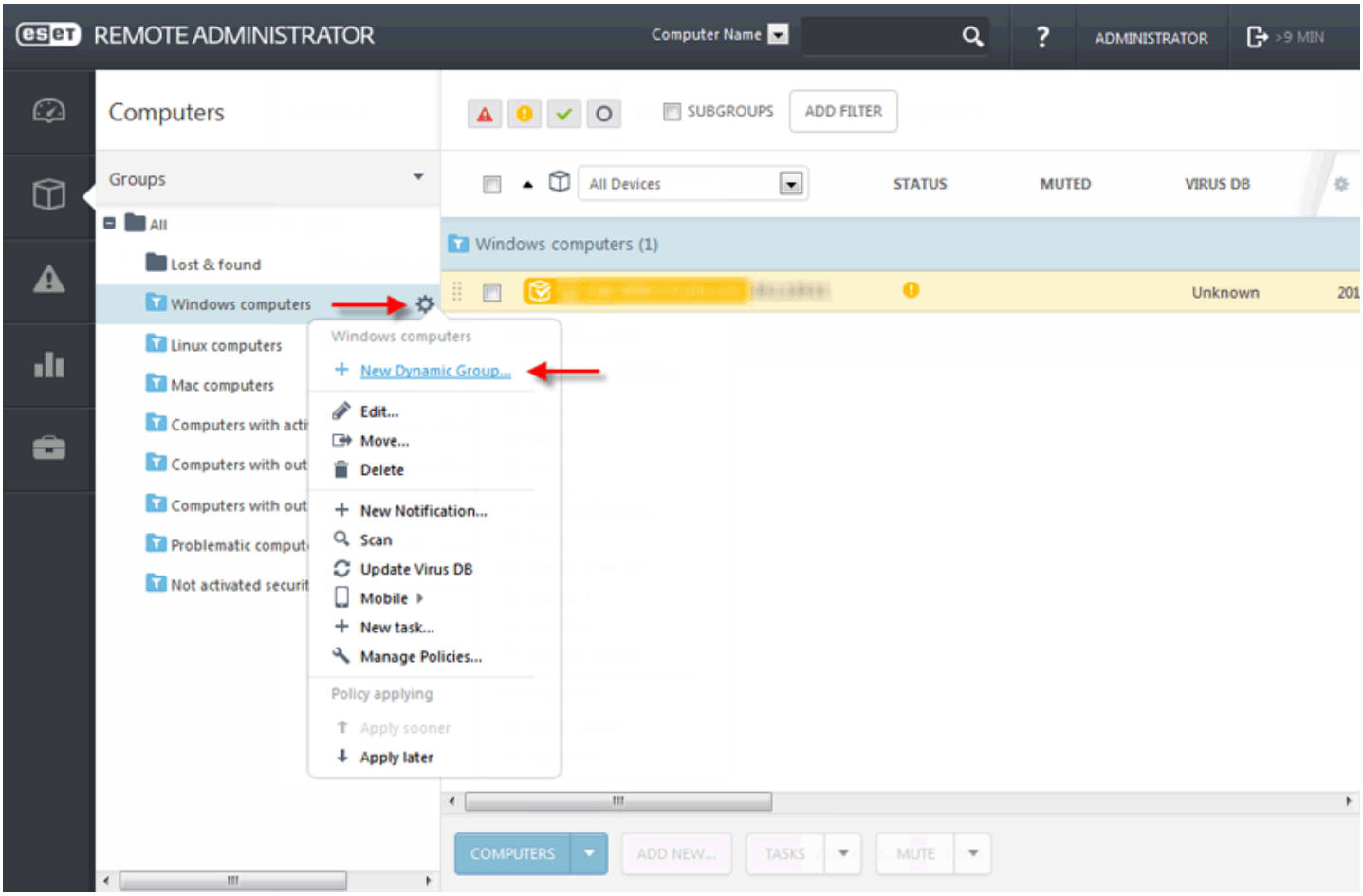
Enter a **Name** and **Description** (optional) for the new Static Group. By default, the parent group is the group you selected when you started creating the New Static Group. If you want to change its parent group, click **Change Parent Group** and select a parent group from the tree. The parent of the New Static Group must be a Static Group. This is because it is not possible for a Dynamic Group to have Static Groups. Click **Finish** to create the New Static Group.



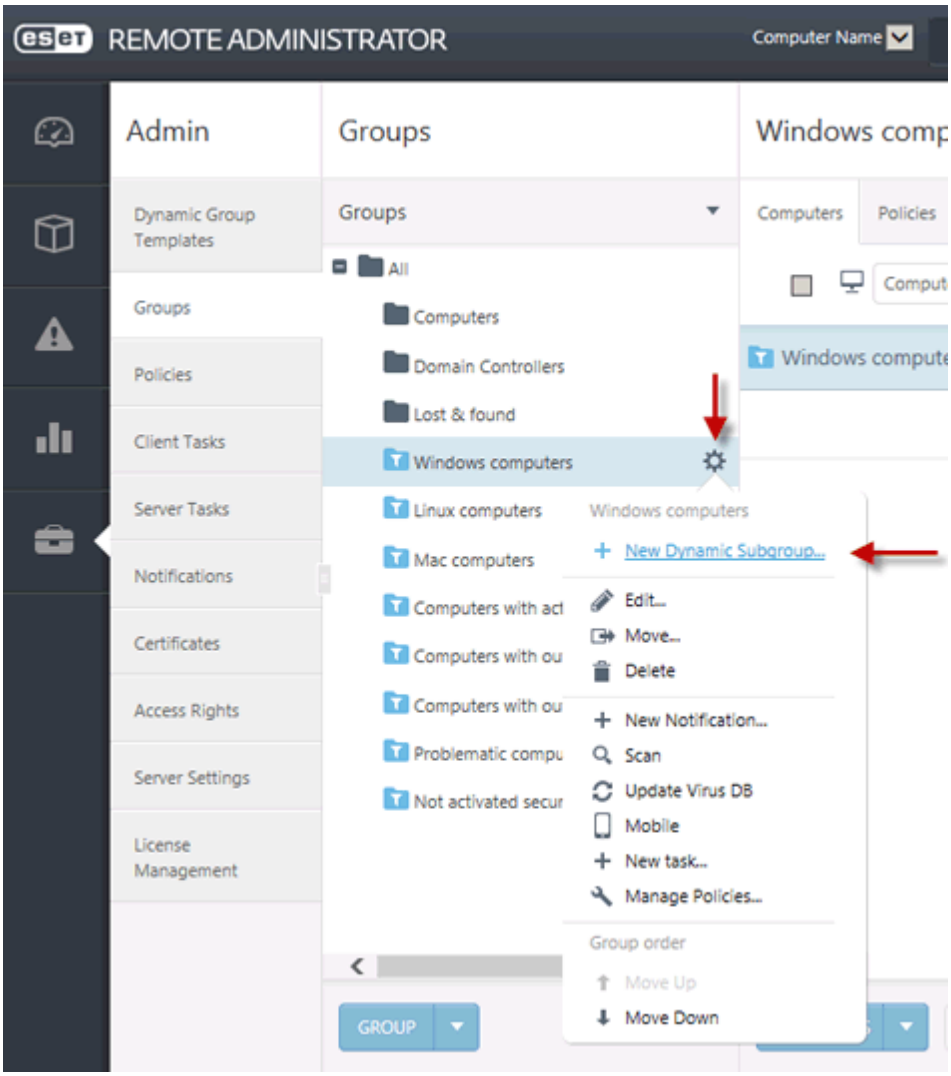
6.1.1.2 Create new Dynamic Group

There are three ways to create a New Dynamic Group:

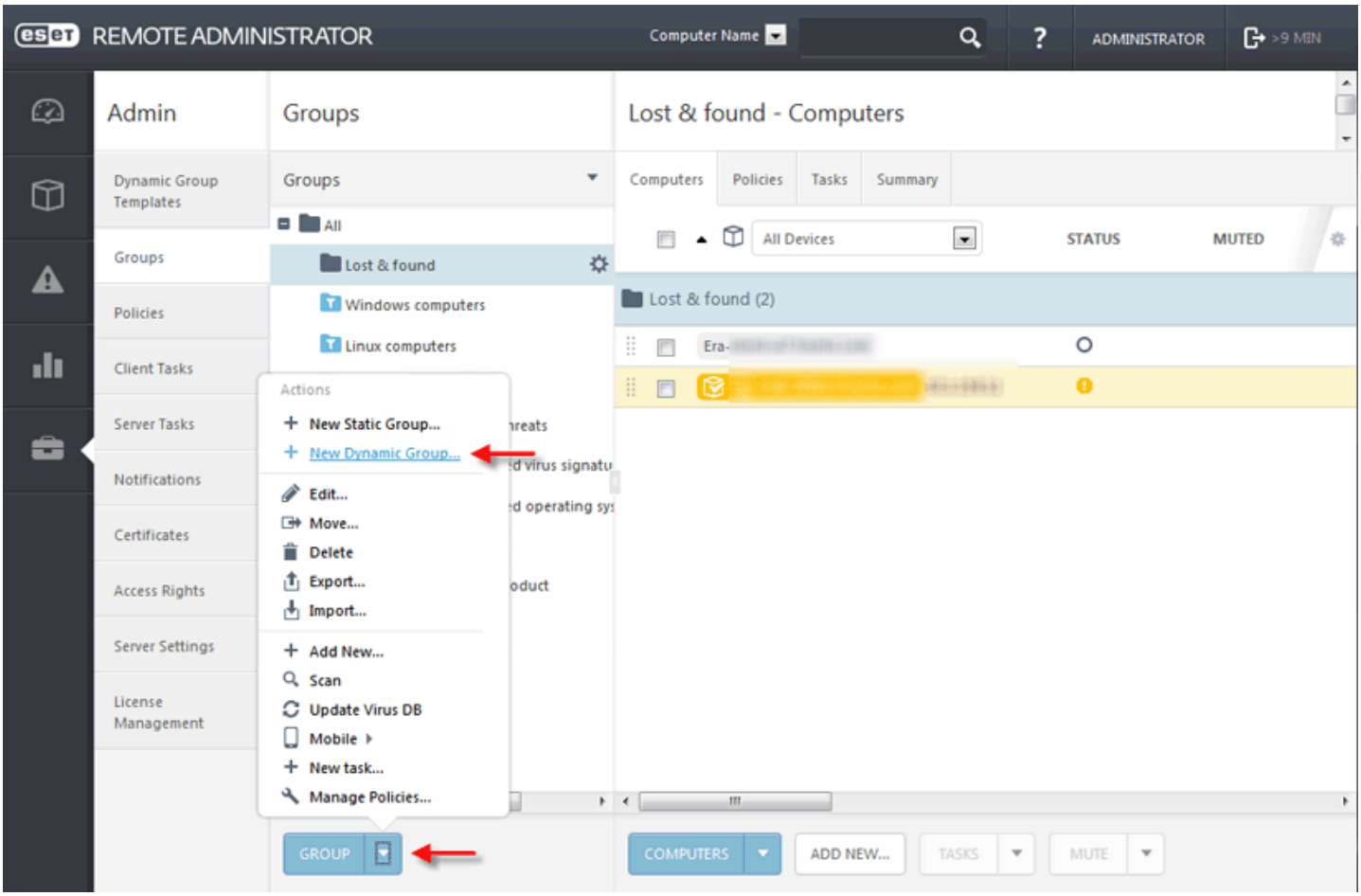
1. Click **Computers** > **Groups** > ⚙ and select **New Dynamic Group...**



2. Click **Admin** > **Groups** > ⚙ > **New Dynamic Subgroup...**



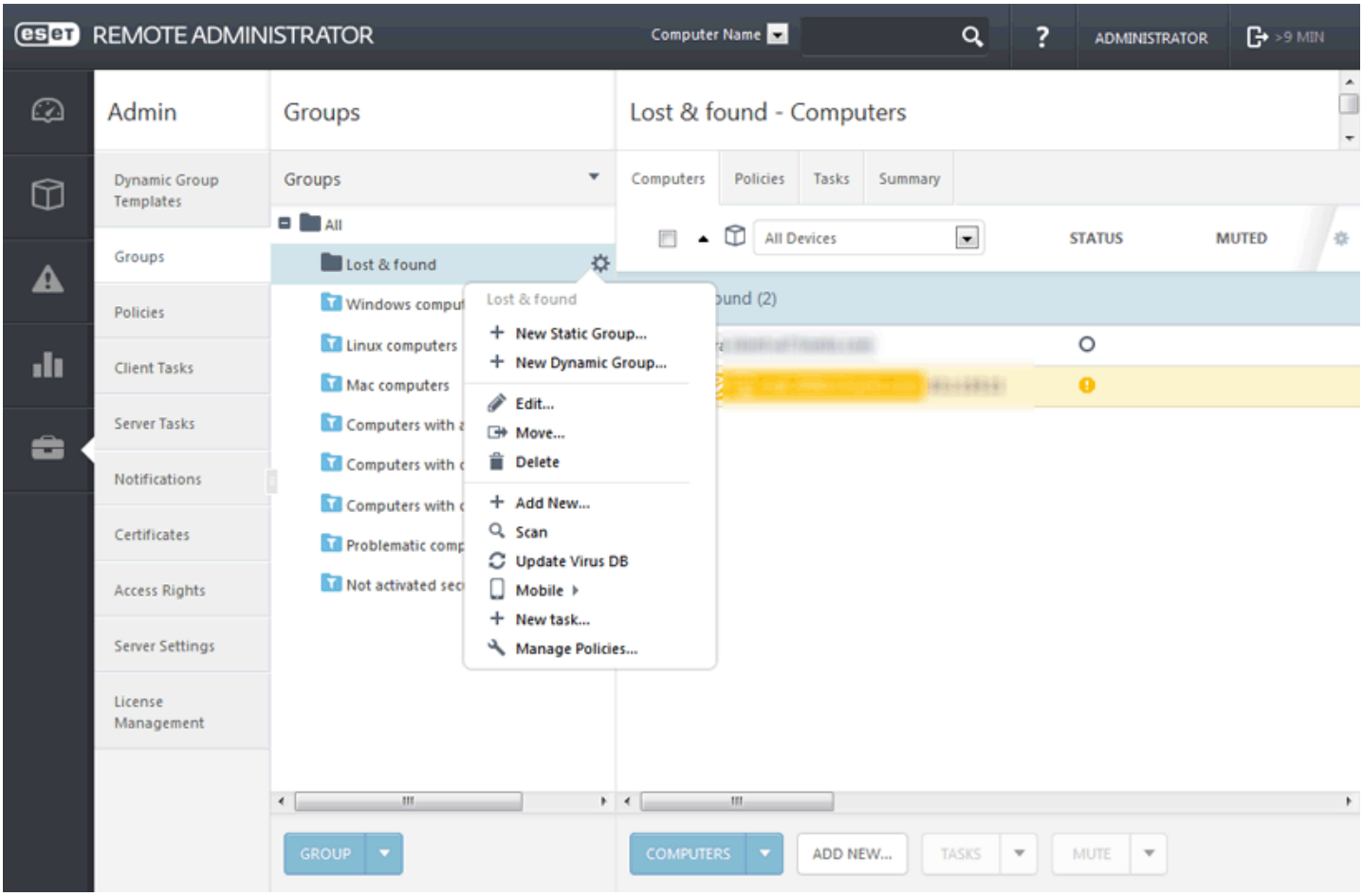
3. Click **Admin** > **Groups** > Click the **Group** button and click **New Dynamic Group...**



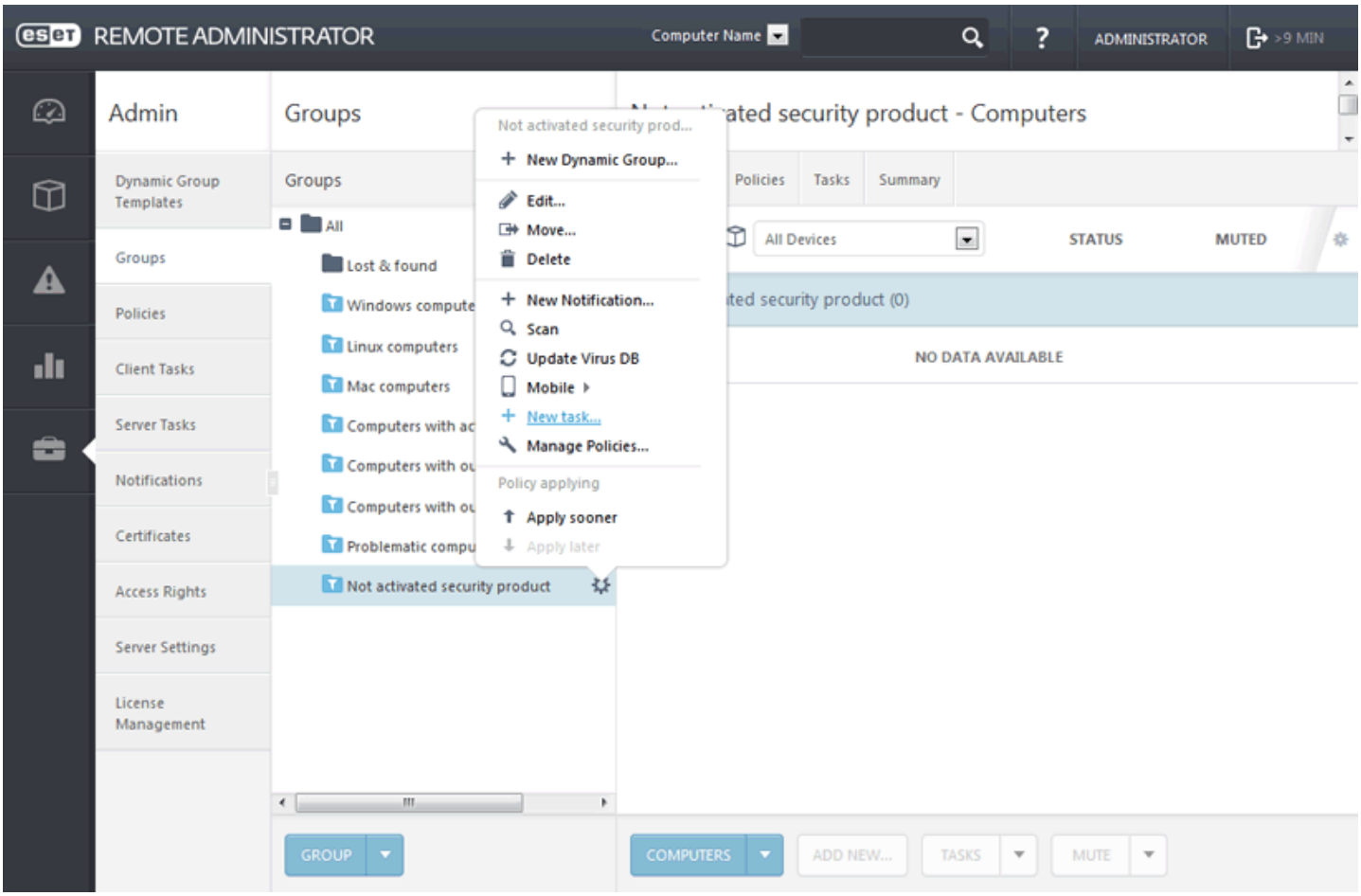
A New Dynamic Group Wizard will appear.

6.1.1.3 Assign Task to a Group

Click **Admin** > **Groups** > select **Static** or **Dynamic** group > ⚙ next to the selected group, or click **Group** > **+ New task**



The same can be done from **Computers**, select **Static** or **Dynamic** and click ⚙ > **+ New task**

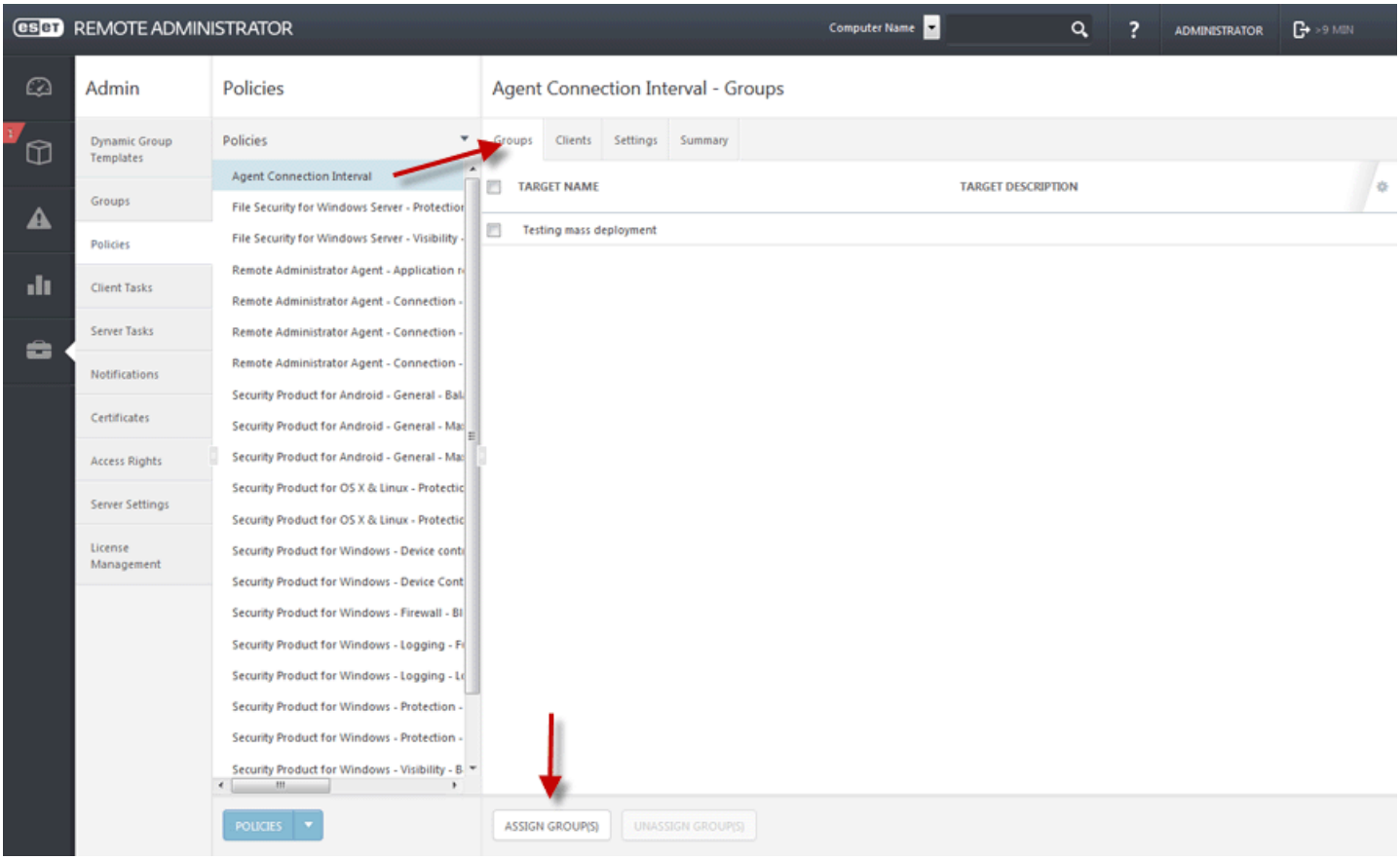


A New Client task wizard window will open.

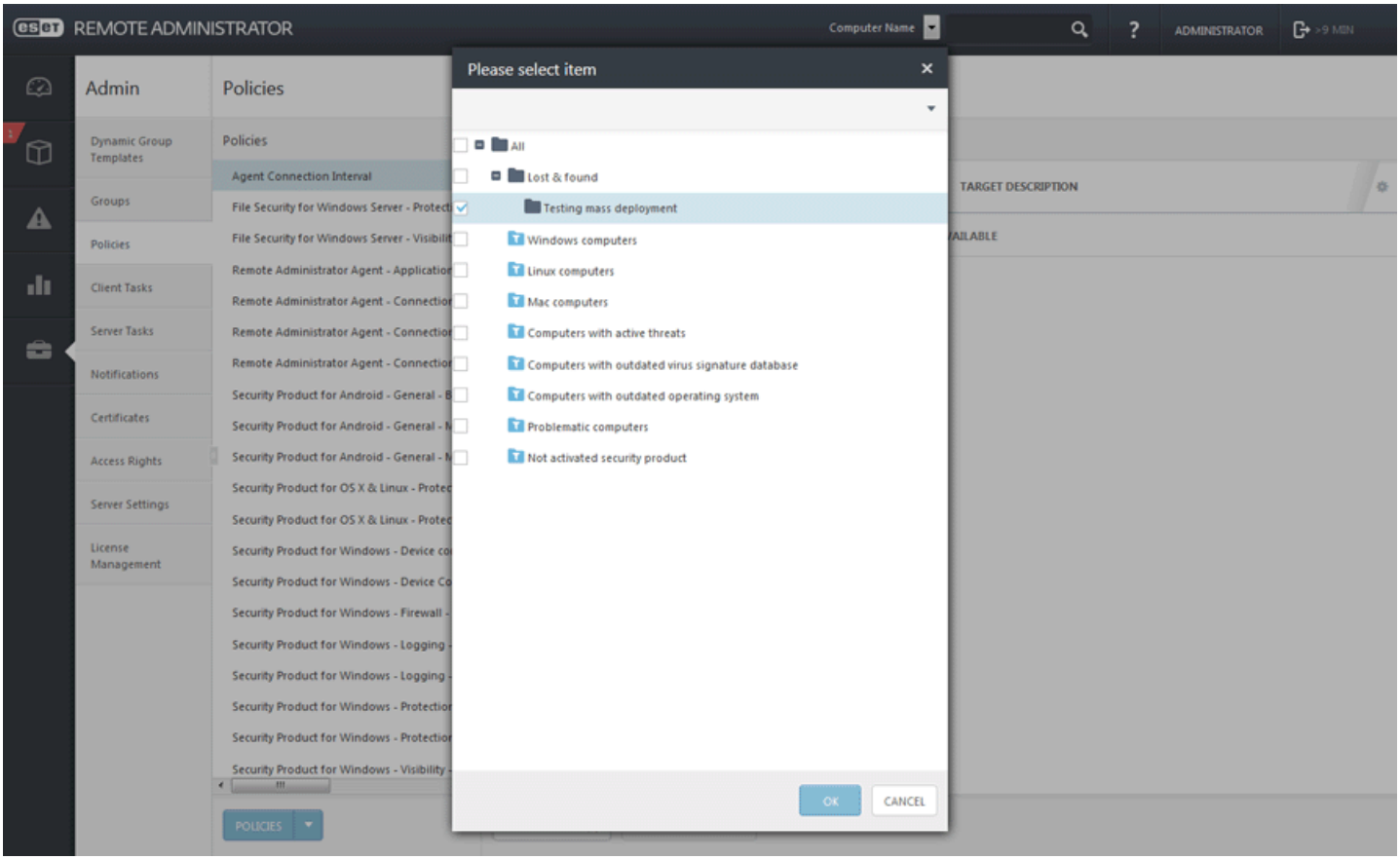
6.1.1.4 Assign a Policy to a Group

After a Policy is created, you can assign it to a **Static** or **Dynamic Group**. There are a two ways to assign a policy:

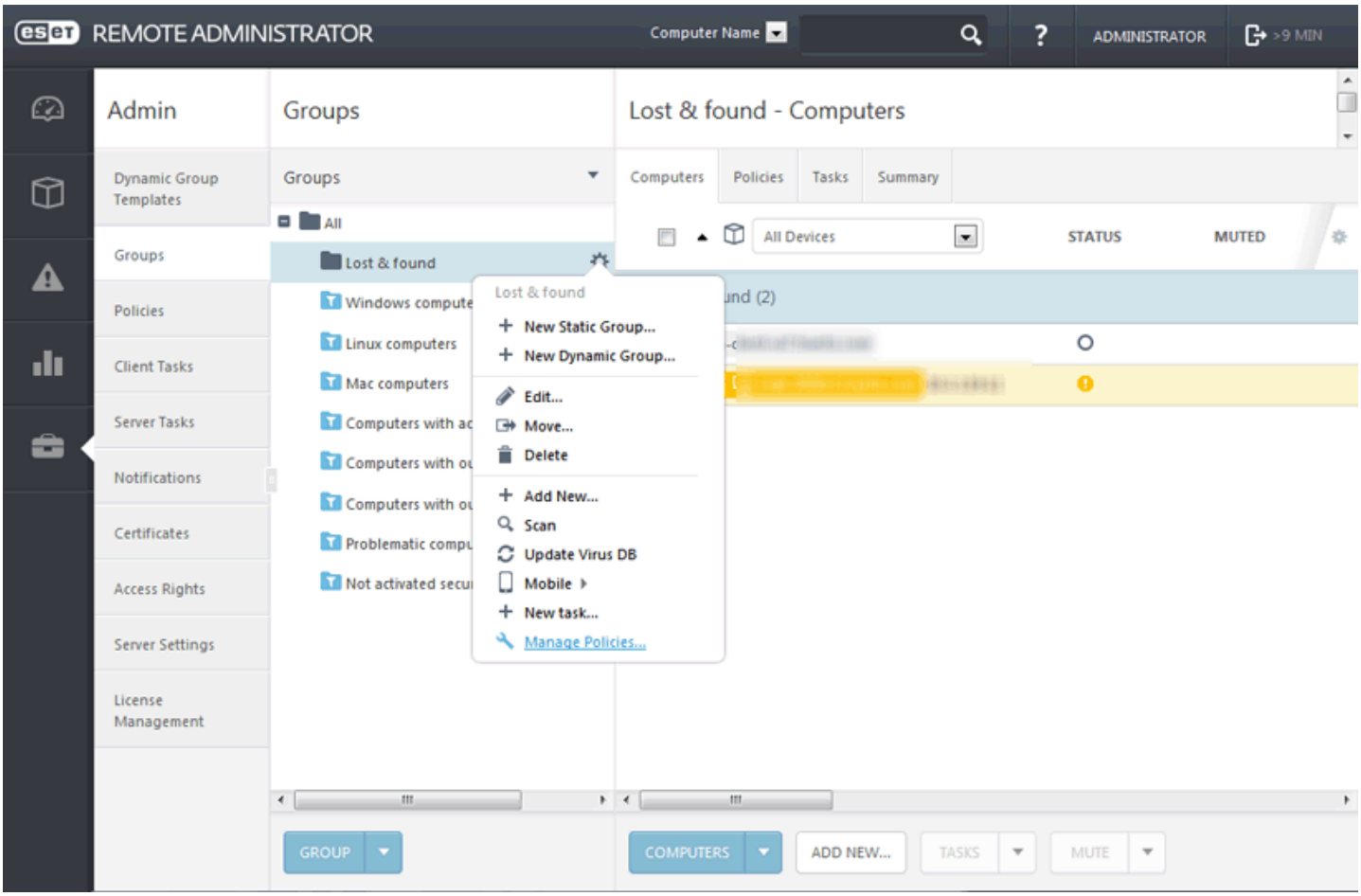
1. Under **Admin** > **Policies** > select a policy and click **Assign Group(s)**. Select a Static or Dynamic Group and click **OK**.



Select **Group** from the list.



2. Click **Admin** > **Groups** > **Group** or click the cogwheel icon next to the group name and select **Manage Policies**.



In the **Policy application order** window click **Add Policy**. Select the check box next to the policy that you want to assign to this group and click **OK**.
Click **Save**. To see what policies are assigned to a particular group, select that group and click the **Policies** tab to view a list of policies assigned to the group.

NOTE: For more information about policies, see the Policies chapter.

6.1.1.5 Policies and Groups

Membership of a computer in Dynamic Group is determined by policies assigned to this computer. It is also determined by the template on which the Dynamic Group is based.

6.1.1.6 Static Groups

- Static Groups are used to manually sort client computers into **groups** and **subgroups**. You can create custom Static Groups and move desired computers into them.
- Static Groups can be created only manually. Client computers can then be moved manually into these groups. Each computer can belong only to one Static Group.

There are two default Static Groups:

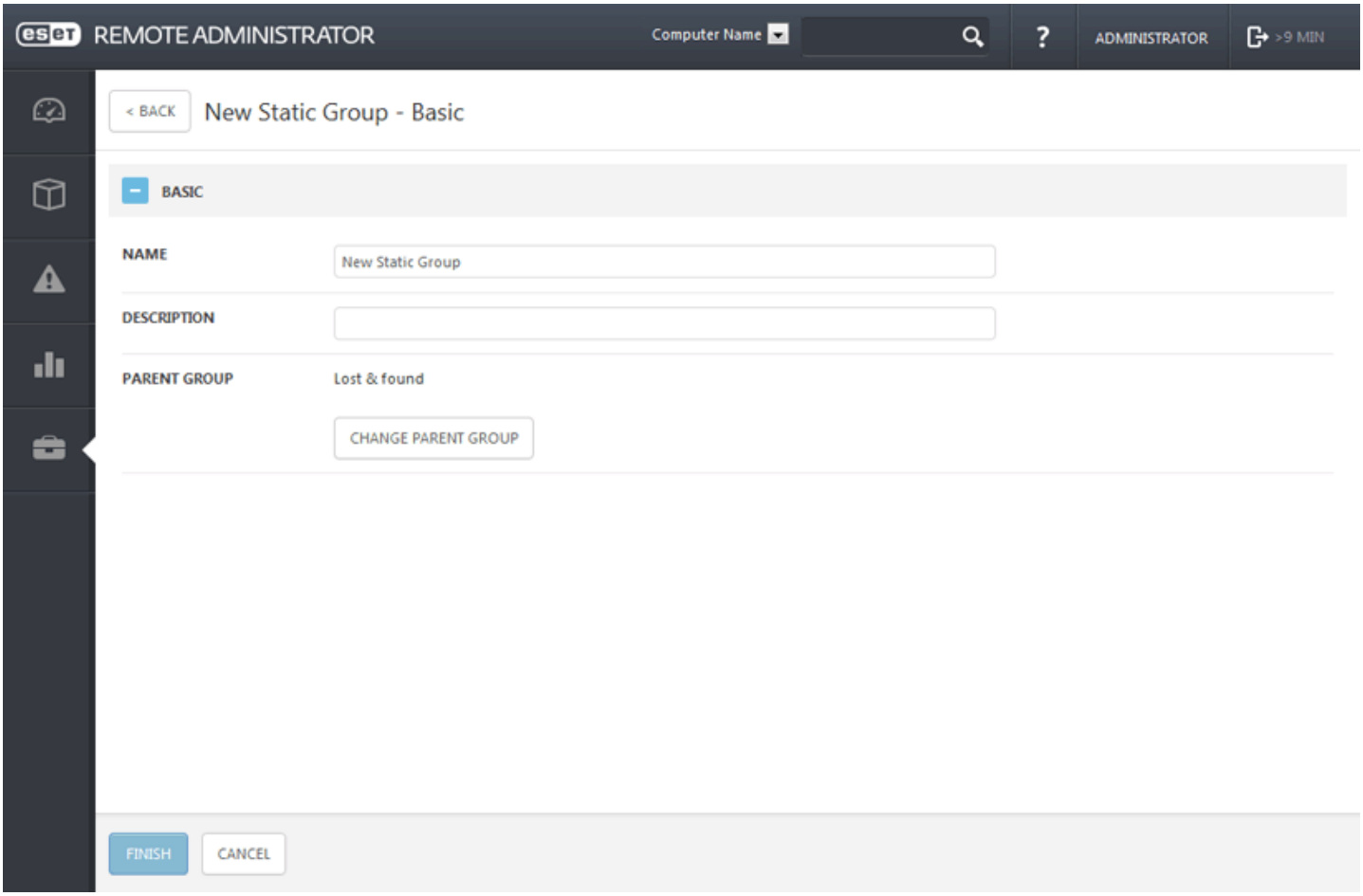
- **All -** This is a main group for all computers in ERA Servers network. It is used for applying of Policies for each computer as a default policy. The group is always displayed and it is not allowed to change Groups name by editing the group.
- **Lost & Found** as a child group of group **All** - Each new computer that first time connects with Agent to server is automatically displayed in this group. The group can be renamed, copied but it can't be deleted or moved.

6.1.1.6.1 Static Group Wizard

Under **Computers** > **Groups** select one of the Static Groups, click the cogwheel and then select **New Static Group.**

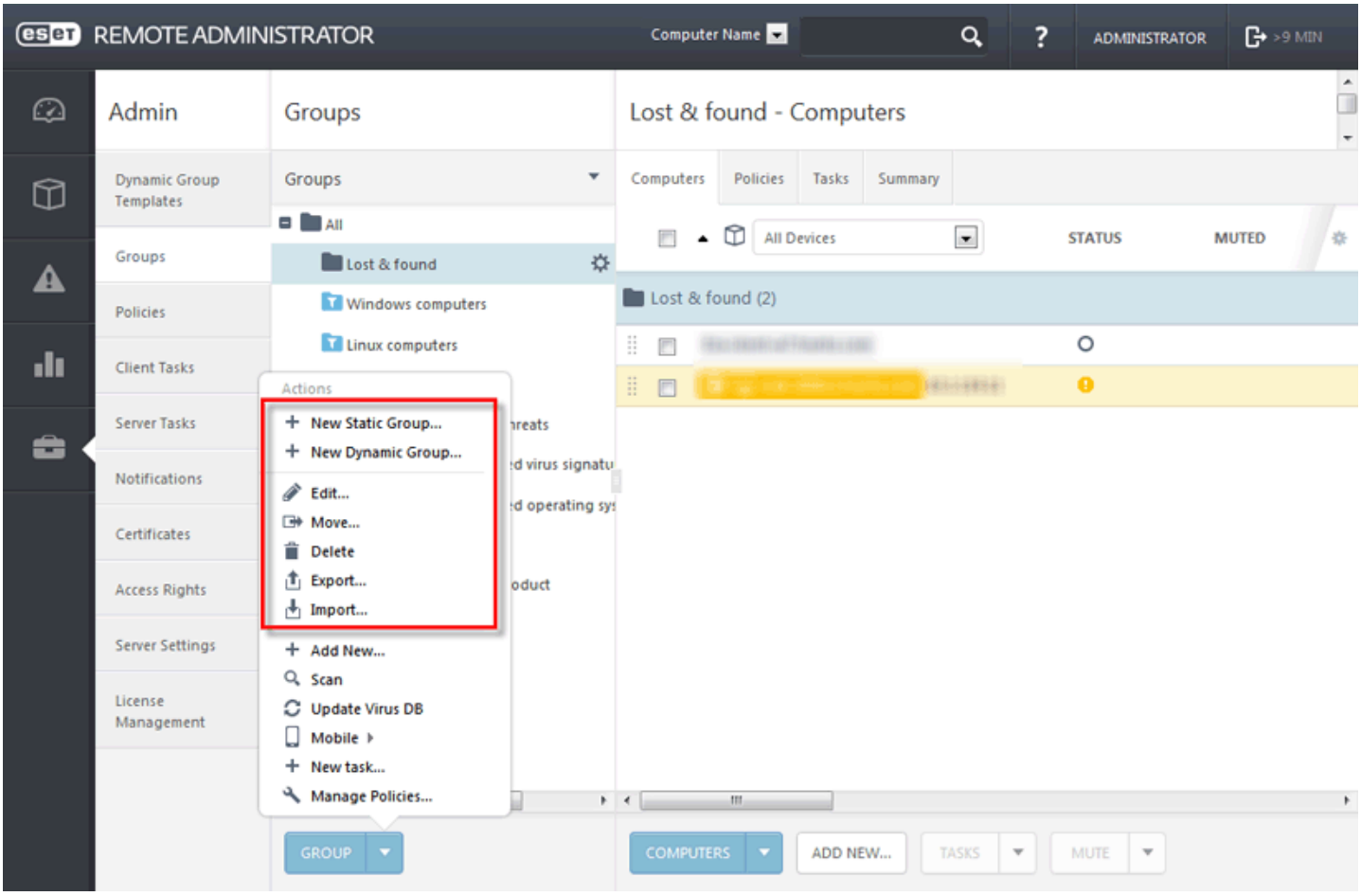
Basic

Enter a **Name** and a **Description** for the new group. Optionally, you can change the **parent group**. By default, the parent group is the group that you selected when you created the New Static Group. Click **Finish** to create the New Static Group.



6.1.1.6.2 Manage Static Groups

Navigate to **Admin** > **Groups** and select the Static Group you want to manage. Click the **Group** button or the cogwheel ⚙ next to the Static Group name. A popover menu will open with available options:



New static group
The Static Group you selected when clicking the **Group** button or the cogwheel ⚙ will be the default parent group, but you can change the parent group later (if needed) when you create a new Static Group.

Edit Group
Allows you to edit the selected group. The same settings apply as when creating a new group (static or dynamic).

Move
Allows you to move the selected group to another group. The group you moved will become a subgroup of that group.

Delete
Removes the selected group completely.

Export
Export members of the group (and subgroups, if selected) to a list (*.txt* file). This list can be used for review or imported later.

Import
You can import a list (usually a text file) of computers as members of the selected group.

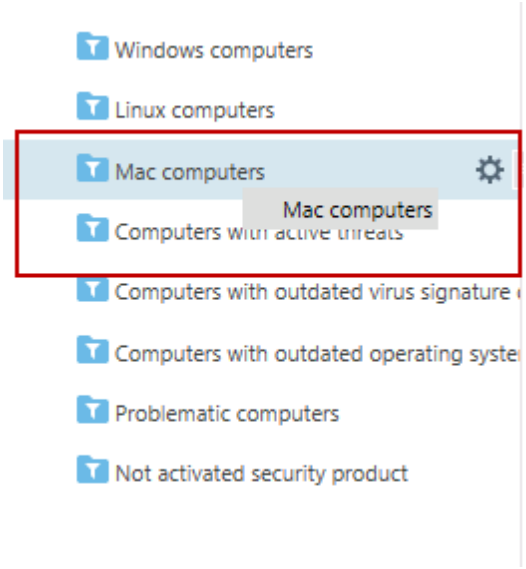
6.1.1.6.3 Move Static Group

Click the cogwheel ⚙ symbol next to the group name and select **Move**. A pop-up window will be displayed showing the groups tree structure. Select the target group (static or dynamic) into which you want to move the selected group. The target group will become a parent group. You can also move groups by dragging and dropping a group into the target group of your choice.

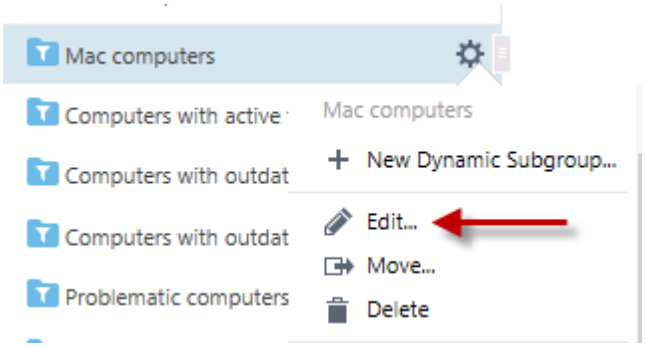
A few exceptions to group organization should be noted. **You cannot move a Static Group into a Dynamic Group**. Also, it is not possible to move pre-defined Static Groups (for example, Lost & found) to any other group. Other groups can be moved freely. A Dynamic Group can be a member of any other group including Static Groups.

The following methods can be used when moving groups:

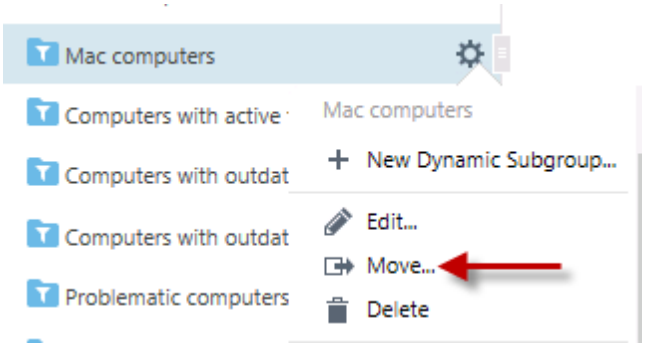
Drag and drop - click and hold the group you want to move and release it above new parent group.



⚙ > **Edit** > **Change parent group**.



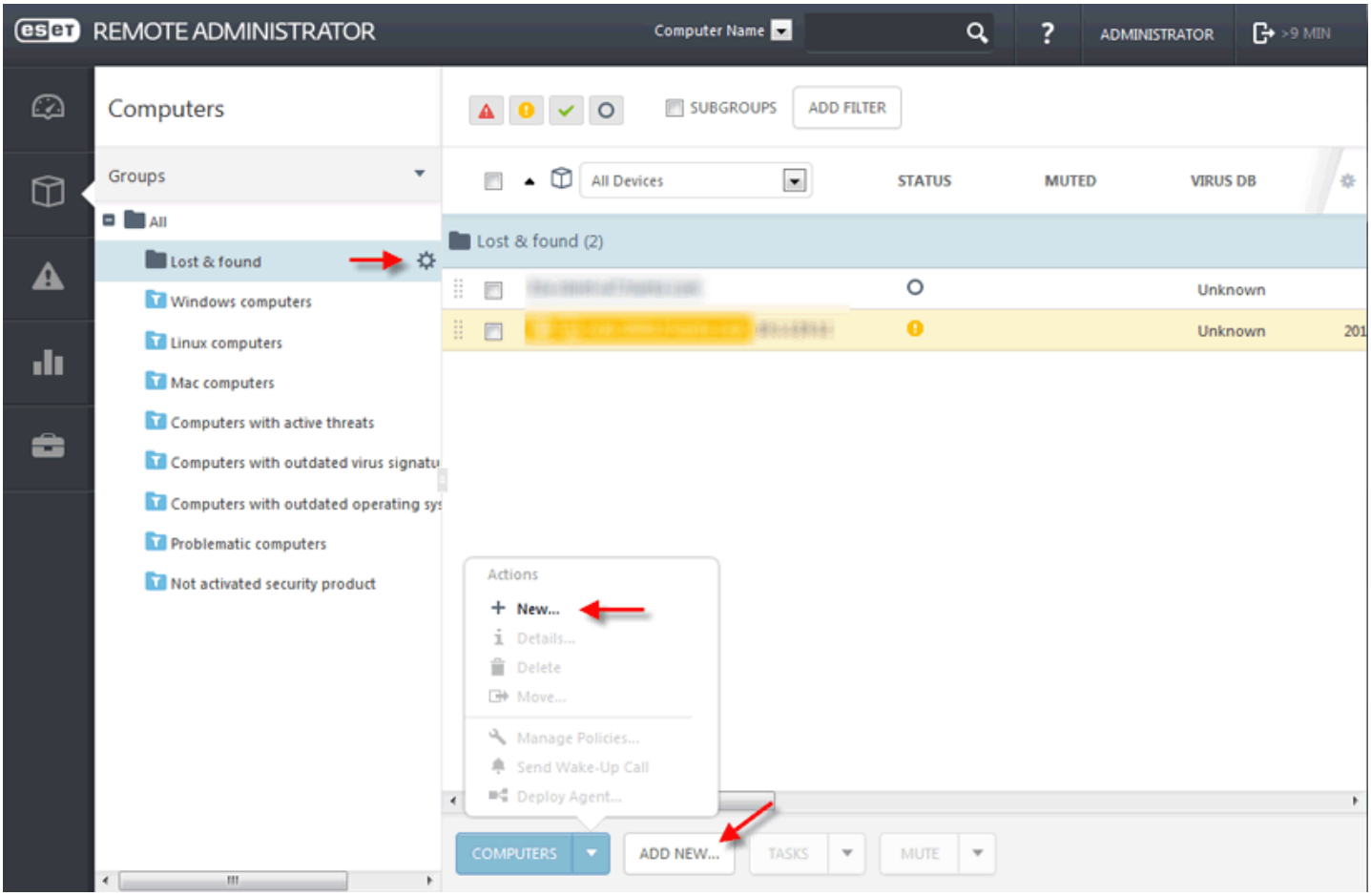
⚙ > **Move** > select a new parent group from the list and click **OK**.



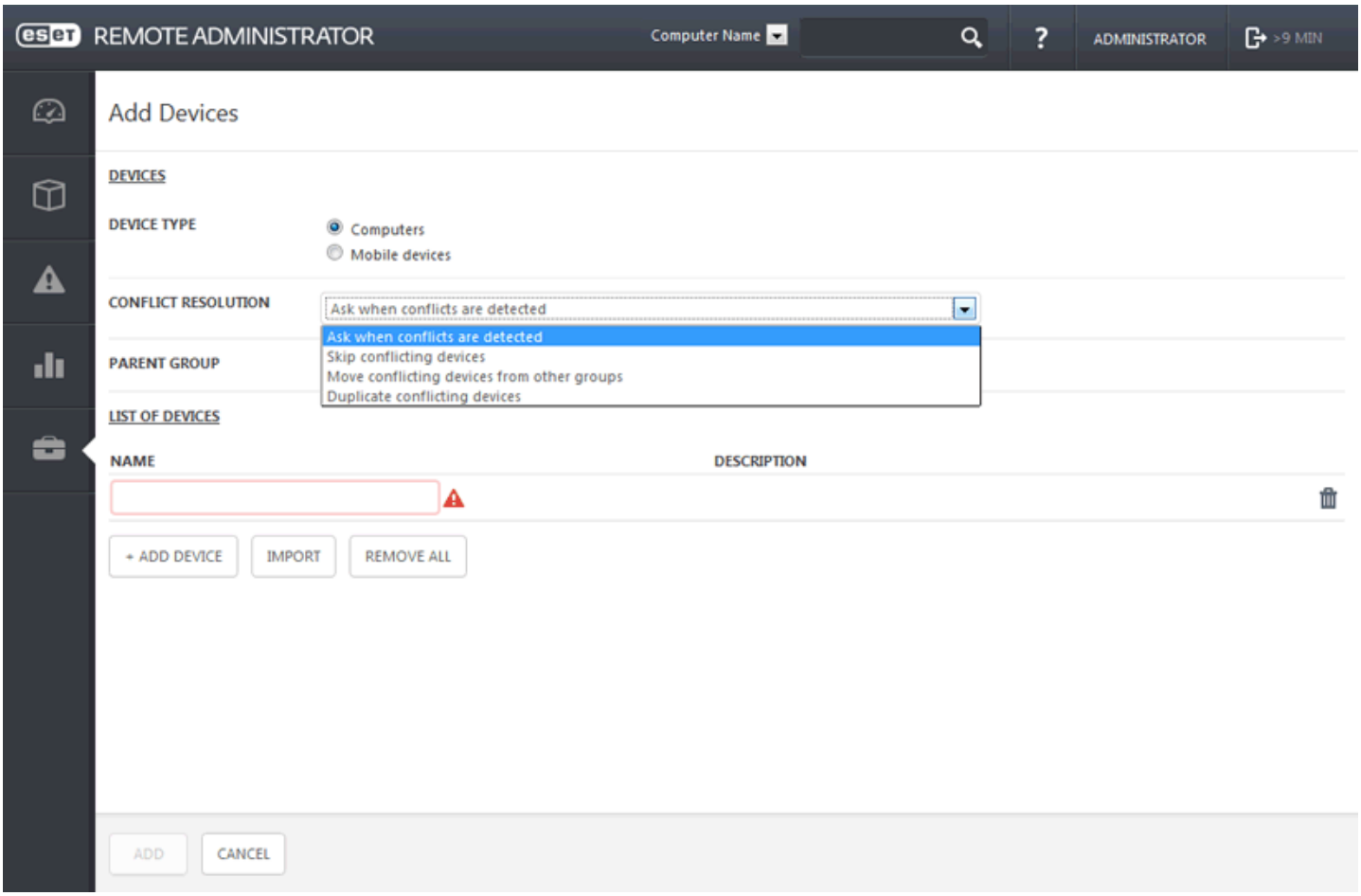
6.1.1.6.4 Add Client Computer to Static Group

Create New Static Group or select one of the default Static Groups.

From the **Computers** tab there are three ways to add new computers. For example, select a Static Group, click the cogwheel icon and select + **Add New**.



Type the name of the computer you want to add into the **Name** field. Click + **Add Device** to add additional computers or click Import to import a file with a list of computers to add. Optionally, you can enter a **description** of the computers.



Use the **Conflict Resolution** drop-down menu to select the action to take if a computer you are adding already exists in ERA:

Ask when conflicts are detected: When a conflict is detected, the program will ask you to select an action (see the options below).
Skip conflicting computers: Duplicate computers will not be added.
Move conflicting computers from other groups: Conflicting computers will be moved from their original groups to the **All** group.
Duplicate conflicting computers: New computers will be added, but with different names.

Click **Add**. Computers can be viewed in the list on the right when you select the group they belong to.

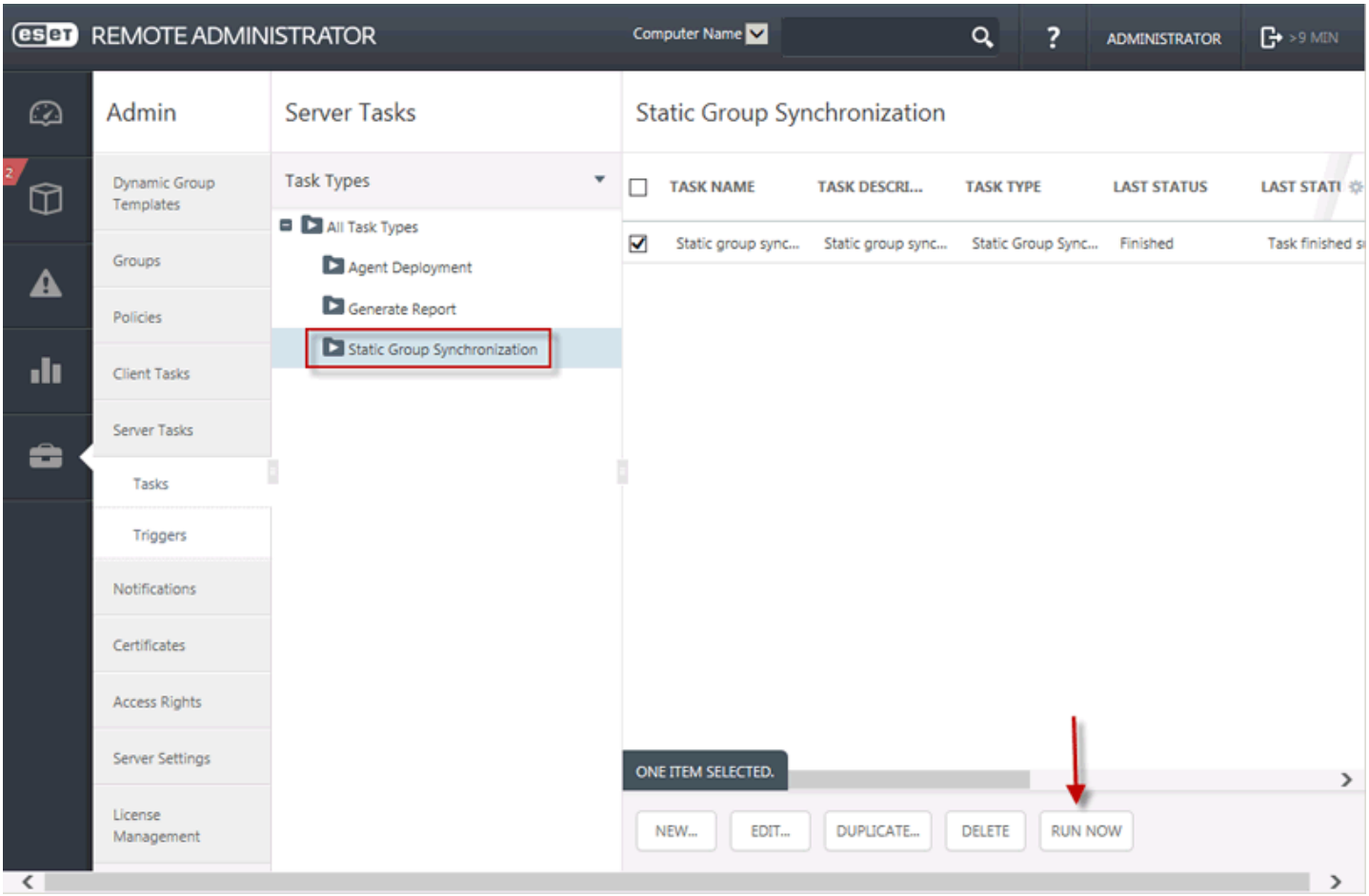
NOTE: Adding multiple computers may take a longer time, reverse DNS lookup may be preformed.

For more information how to add Mobile devices see chapter Mobile device enrollment.

6.1.1.6.5 Import clients from Active Directory

AD synchronization is performed by running the **Static Group Synchronization** server task.

Admin > **Server Task** is a pre-defined default task that you can choose to execute automatically during ESET Remote Administrator installation. If the computer is in a domain, synchronization will be performed and computers from the AD will be listed in a default group **All**.



To start the synchronization process just click the task and choose **Run now**. If you need to create a new AD synchronization task, select a group to which you want to add new computers from the AD. Also select objects in the AD you want to synchronize from and what to do with duplicates. Enter your AD server connection settings and set the **Synchronization mode** to **Active Directory/Open Directory/LDAP**.

Follow step-by-step instructions in this ESET Knowledgebase article.

6.1.1.6.6 Assign a Task to a Static Group

Both Static and Dynamic Groups are treated the same way with regard to task assignment. For instructions on how to assign a task to a group, click here.

6.1.1.6.7 Assign a Policy to a Static Group

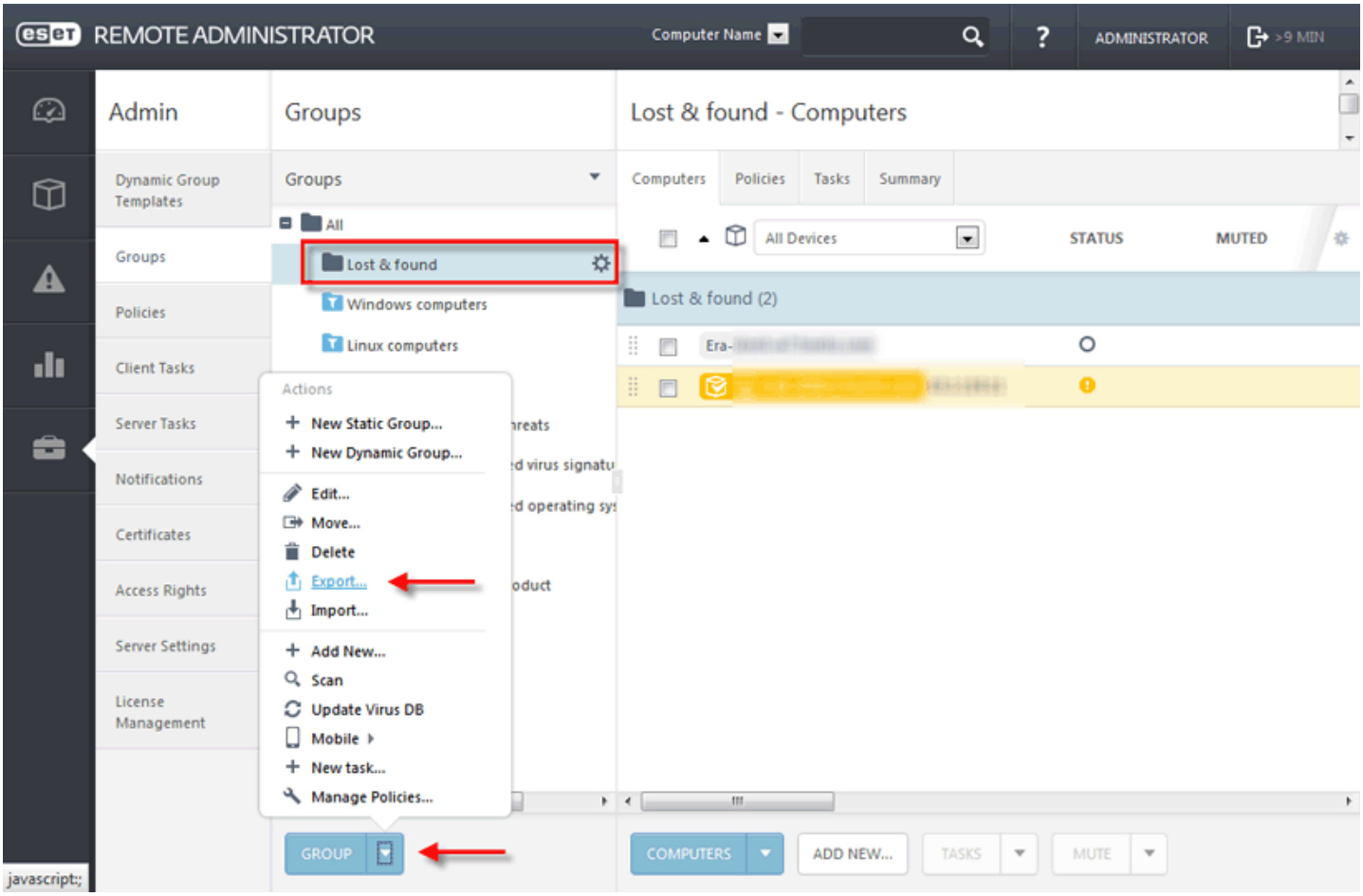
Both Static and Dynamic Groups are treated the same way when it comes to policy assignment. For instructions on how to assign a policy to a group, click here.

6.1.1.6.8 Export Static Groups

Exporting a list of computers that are in the ERA structure is simple. You can export the list and store it as a backup so that you can import the list back in the future, for example if you want to restore the group structure.

NOTE: Static groups need to contain at least one computer. Exporting empty groups is not possible.

1. Go to **Admin** > **Groups** > select a Static Group you want to export.

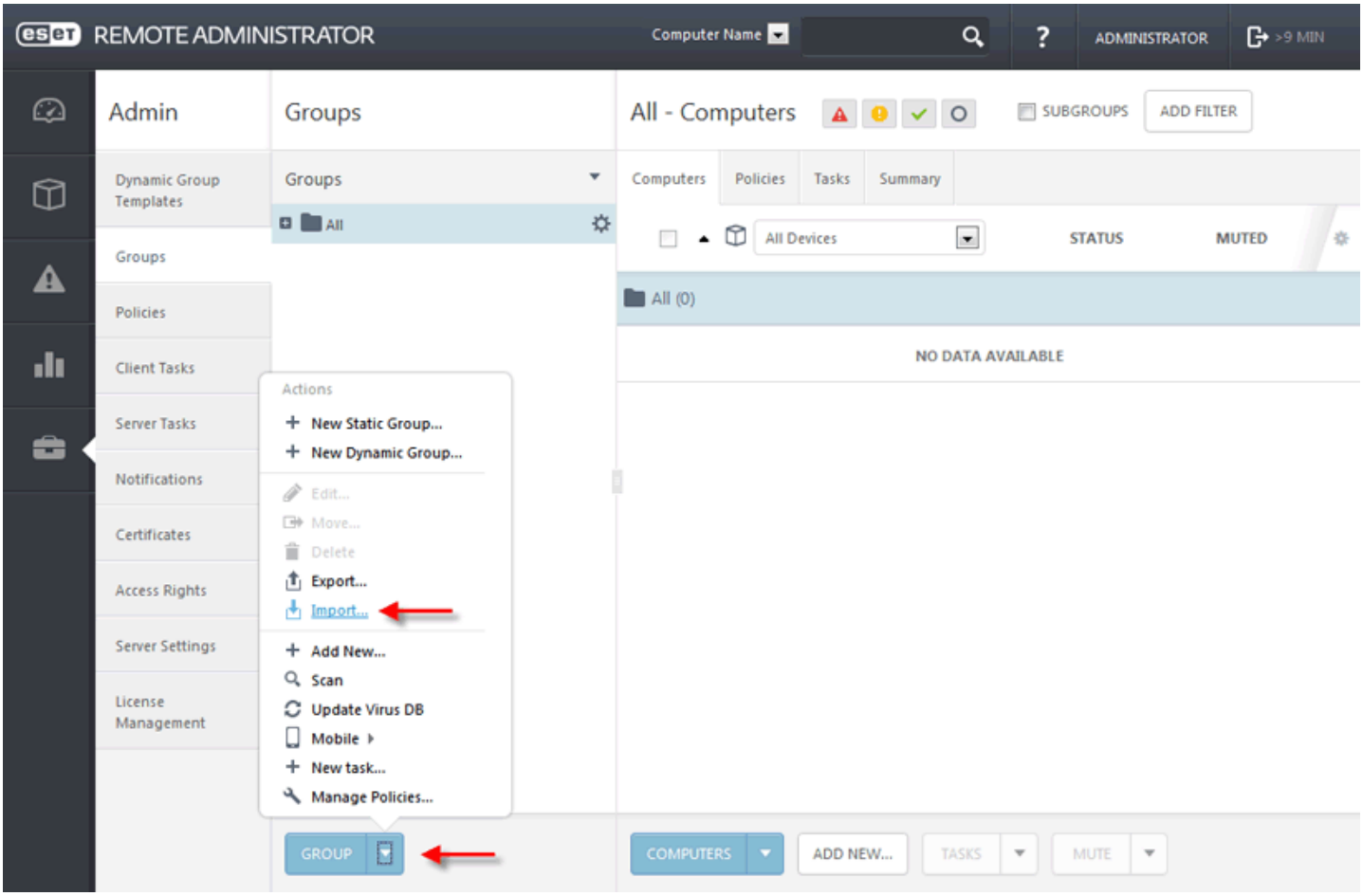


2. Click the **Group** button at the bottom (a context menu will pop-up).
3. Select **Export.**
4. The file will be saved in **.txt** format.

NOTE: Dynamic Groups cannot be exported because Dynamic Groups are only links to computers according to the criteria defined in Dynamic Group Templates.

6.1.1.6.9 Import Static Groups

Exported files from Static Groups can be imported back into ERA Web Console and included in your existing group structure.



1. Click **Group** (a context menu will pop-up).
2. Select **Import**.
3. Click **Browse** and navigate to the **.txt** file.
4. Select the group file and click **Open.** The file name is displayed in the text box.
5. Select one of the following options to resolve conflicts:

- **Skip conflicting computers**

If static Groups exist and computers from the .txt file already exist in this group, those computers are skipped and are not imported. Information about this is displayed.

- **Move conflicting computers from other groups**

If Static Groups exist and computers from the .txt file already exist in this group, it is necessary to move computers to other Static Groups prior to the import, after the import, these computers will be moved back into original groups where from they had been moved.

- **Duplicate conflicting computers**

If Static Groups exist and computers from the .txt file already exist in this group, duplicates of these computers are created in the same Static Group. The original computer is displayed with full information and the duplicate is displayed with its Computer name only.

5. Click **Import** , Static Groups and computers within will be imported.

6.1.1.7 Dynamic Groups

Dynamic Groups are in essence custom filters defined in Templates. Computers are filtered on the Agent side, so no extra information needs to be transferred to server. The Agent decides on its own which Dynamic Groups a client belongs to, and only notifies the server about this decision. Dynamic Groups have their rules defined in the Dynamic Group Template.

There are some pre-defined Dynamic Groups available after you have installed ESET Remote Administrator. If you need to, you can create custom Dynamic Groups. When creating them, create a template first and then create a Dynamic Group.

Another approach is to create a new Dynamic Group and new template on the fly.

More than one Dynamic Group can be created from one template.

A user can use Dynamic Groups in other parts of ERA. It is possible to assign policies to them or prepare a task for all computers therein.

Dynamic Groups can be under Static Groups or Dynamic Groups. However, the topmost group is always static.

All the Dynamic Groups under a certain Static Group only filter computers of that Static Group no matter how deep they are in the tree. Moreover, for nested Dynamic Groups, a deeper Dynamic Group filters the results of the superior one.

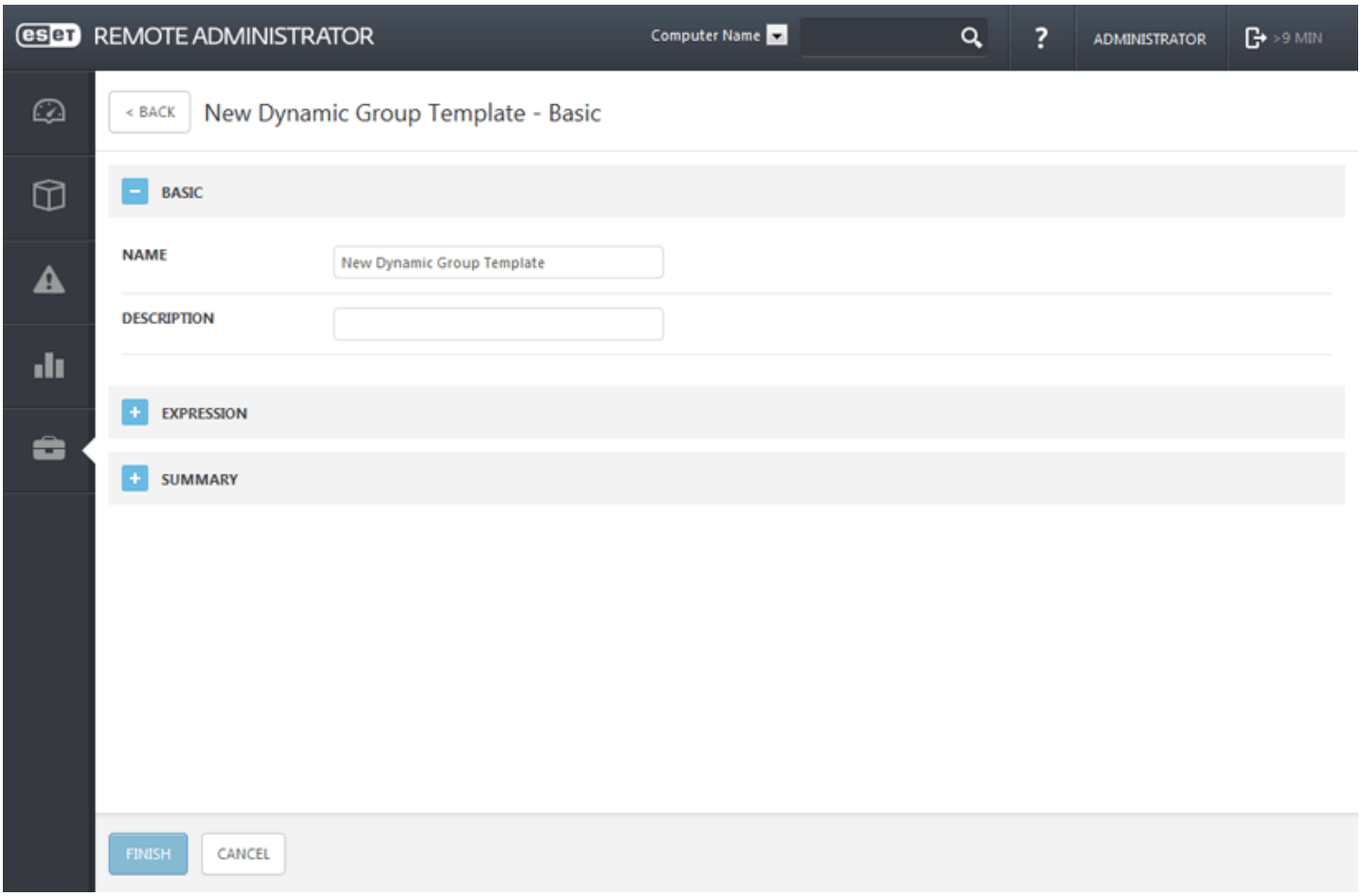
Policies are applied as described here. However, once created, they can be moved freely across the tree.

6.1.1.7.1 Dynamic Group Template Wizard

Click **New Template** under **Admin** > **Dynamic Group Templates.**

Basic

1. Enter a **Name** and a **Description** for the new Dynamic Group template.



Expression

Select a logical operator in the **Operation** menu.

- **AND** - All defined conditions have to be true.
- **OR** - At least one condition has to be true.
- **NAND** - At least one condition has to be false.
- **NOR** - All conditions have to be false.

For example, select **AND**. This means that a computer must meet all conditions in order to appear in a Dynamic Group that uses this template.

- Click **+ Add Rule** and select a condition. Let's say you aim at clients who use laptops that are plugged into electricity. Select **Hardware** > **Running on battery** > **=(equal)** > **Not discharging**.
- Click **+ Add Rule** to enter a second condition (number of rules is not limited). Select **OS edition** > **OS type** > **=(equal)** > **Windows 8.1** (enter this value into the blank field).

If both of these conditions are met, the client will appear in the Dynamic Group.

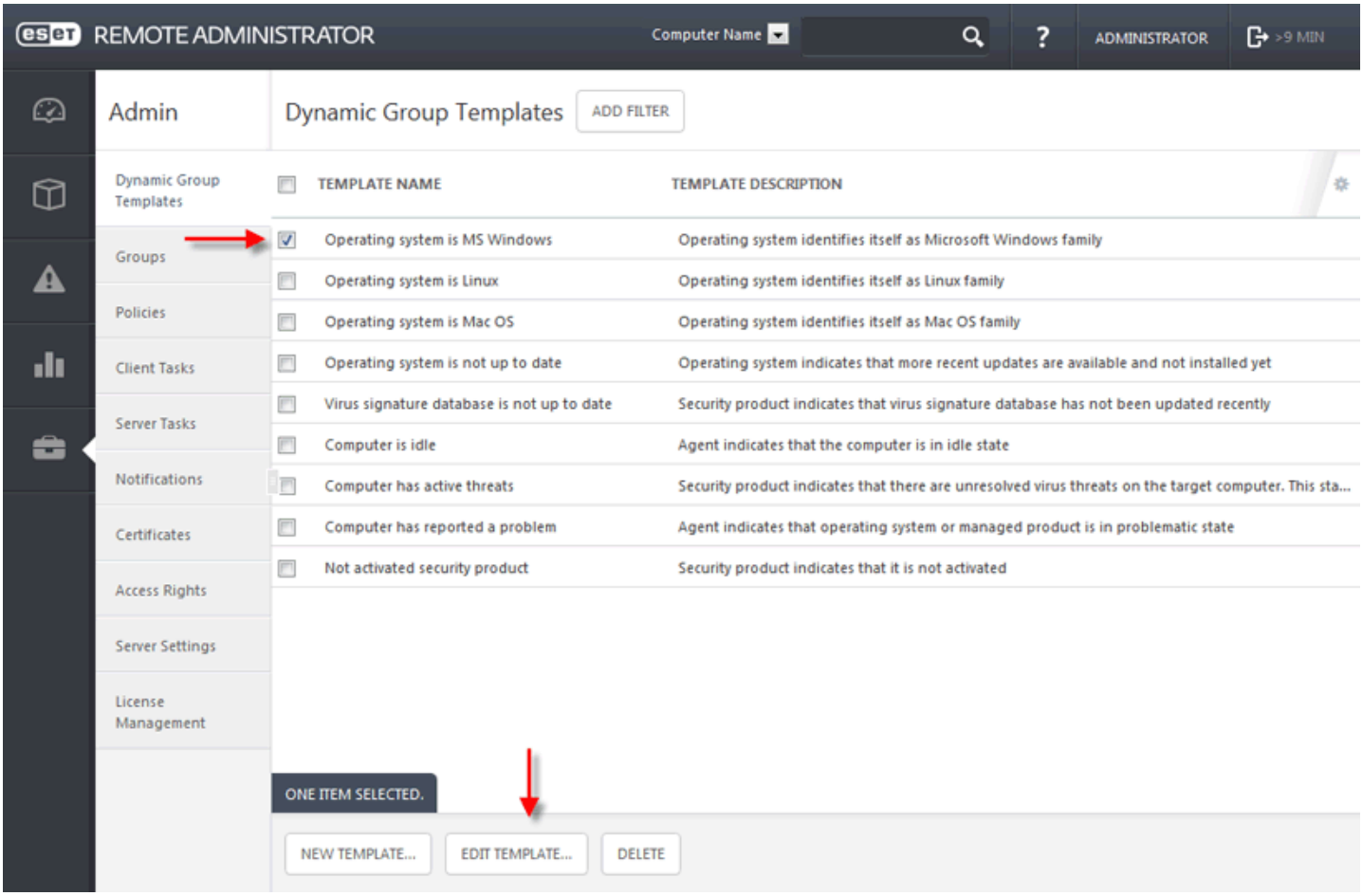
Summary

Review the configured settings and click **Finish** to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.In **Expression** options you can configure rules/conditions for the group (Rule editor is described here). Now, every Dynamic Group based on this template will evaluate these rules.

To save your changes, click **Finish**.

6.1.1.7.2 Manage Dynamic Group Templates

Templates can be managed from **Admin** > **Dynamic Group Templates**.


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
>9 MIN
Admin
Dynamic Group Templates
ADD FILTER
Dynamic Group Templates
Groups
Policies
Client Tasks
Server Tasks
Notifications
Certificates
Access Rights
Server Settings
License Management
TEMPLATE NAME
TEMPLATE DESCRIPTION
Operating system is MS Windows
Operating system identifies itself as Microsoft Windows family
Operating system is Linux
Operating system identifies itself as Linux family
Operating system is Mac OS
Operating system identifies itself as Mac OS family
Operating system is not up to date
Operating system indicates that more recent updates are available and not installed yet
Virus signature database is not up to date
Security product indicates that virus signature database has not been updated recently
Computer is idle
Agent indicates that the computer is in idle state
Computer has active threats
Security product indicates that there are unresolved virus threats on the target computer. This sta...
Computer has reported a problem
Agent indicates that operating system or managed product is in problematic state
Not activated security product
Security product indicates that it is not activated
ONE ITEM SELECTED.
NEW TEMPLATE...
EDIT TEMPLATE...
DELETE

You can either create a New Template or edit any of the existing templates. To edit, click the template you want to edit and a wizard will open. Alternatively, you can select a template by clicking the check box next to it and then clicking **Edit Template**.

Expression

Select a logical operator in the **Operation** menu.

- **AND** - All defined conditions have to be true.
- **OR** - At least one condition has to be true.
- **NAND** - At least one condition has to be false.
- **NOR** - All conditions have to be false.

For example, select **AND**. This means that a computer must meet all conditions in order to appear in a Dynamic Group that uses this template.

- Click **+ Add Rule** and select a condition. Let's say you aim at clients who use laptops that are plugged into electricity. Select **Hardware** > **Running on battery** > **=(equal)** > **Not discharging**.
- Click **+ Add Rule** to enter a second condition (number of rules is not limited). Select **OS edition** > **OS type** > **=(equal)** > **Windows 8.1** (enter this value into the blank field).

If both of these conditions are met, the client will appear in the Dynamic Group.

Summary

Review the configured settings and click **Finish** to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.In **Expression** options you can configure rules/conditions for the group (Rule editor is described here). Now, every Dynamic Group based on this template will evaluate these rules.

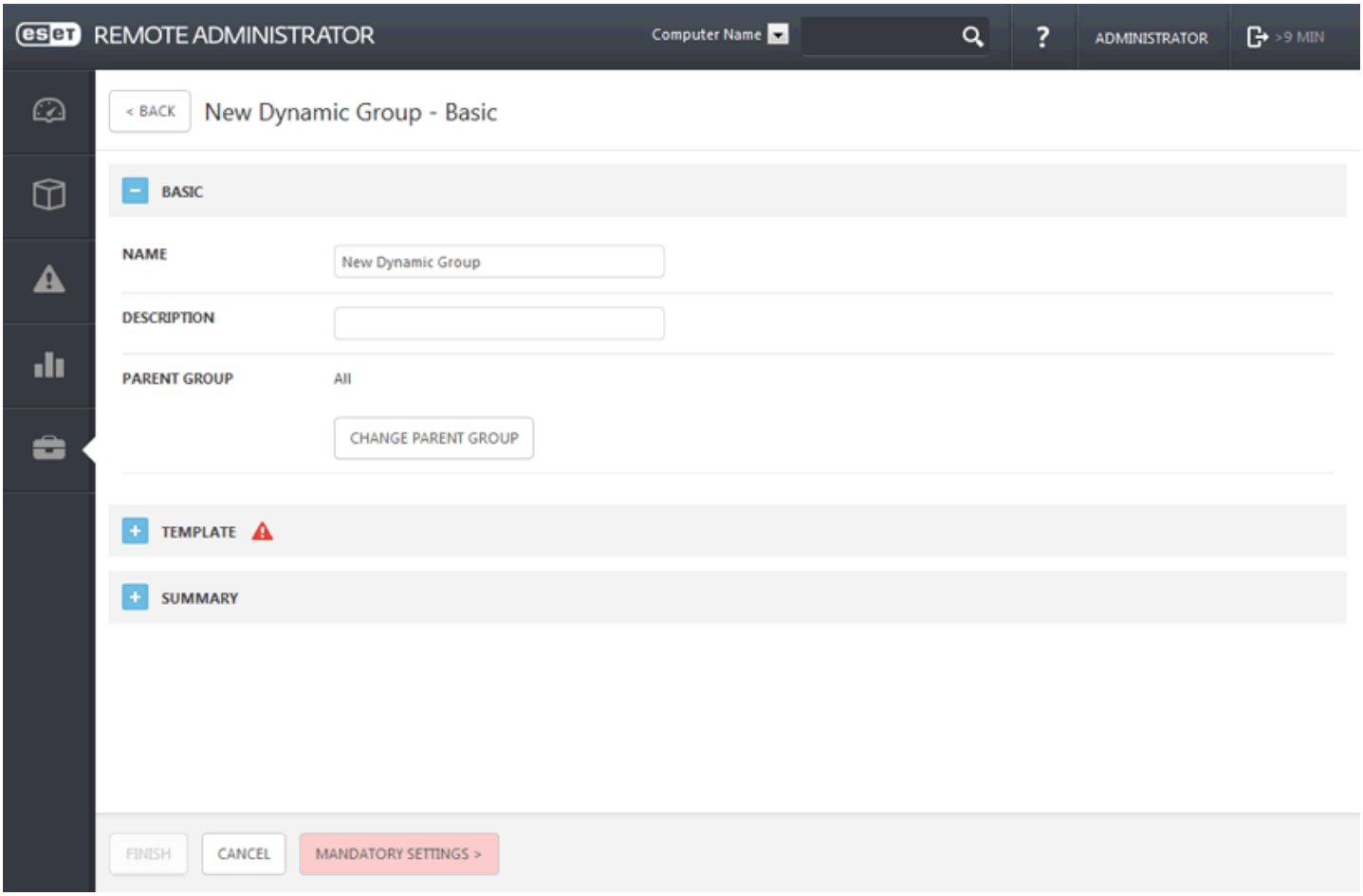
To save your changes, click **Finish**.

6.1.1.7.3 Dynamic Group Wizard

You can create Dynamic Groups using an existing Template or a new template (which will then be used for this Dynamic Group).

Basic

Enter a **Name** and **Description** (optional) for the new Dynamic Group. By default, the parent group is the group you selected when you started creating the new static group. If you want to change its parent group, you can still do so by clicking **Change Parent Group** and selecting one from the tree. The parent of the new dynamic group can be dynamic or static. Click **Finish** to create the new dynamic group.



Template

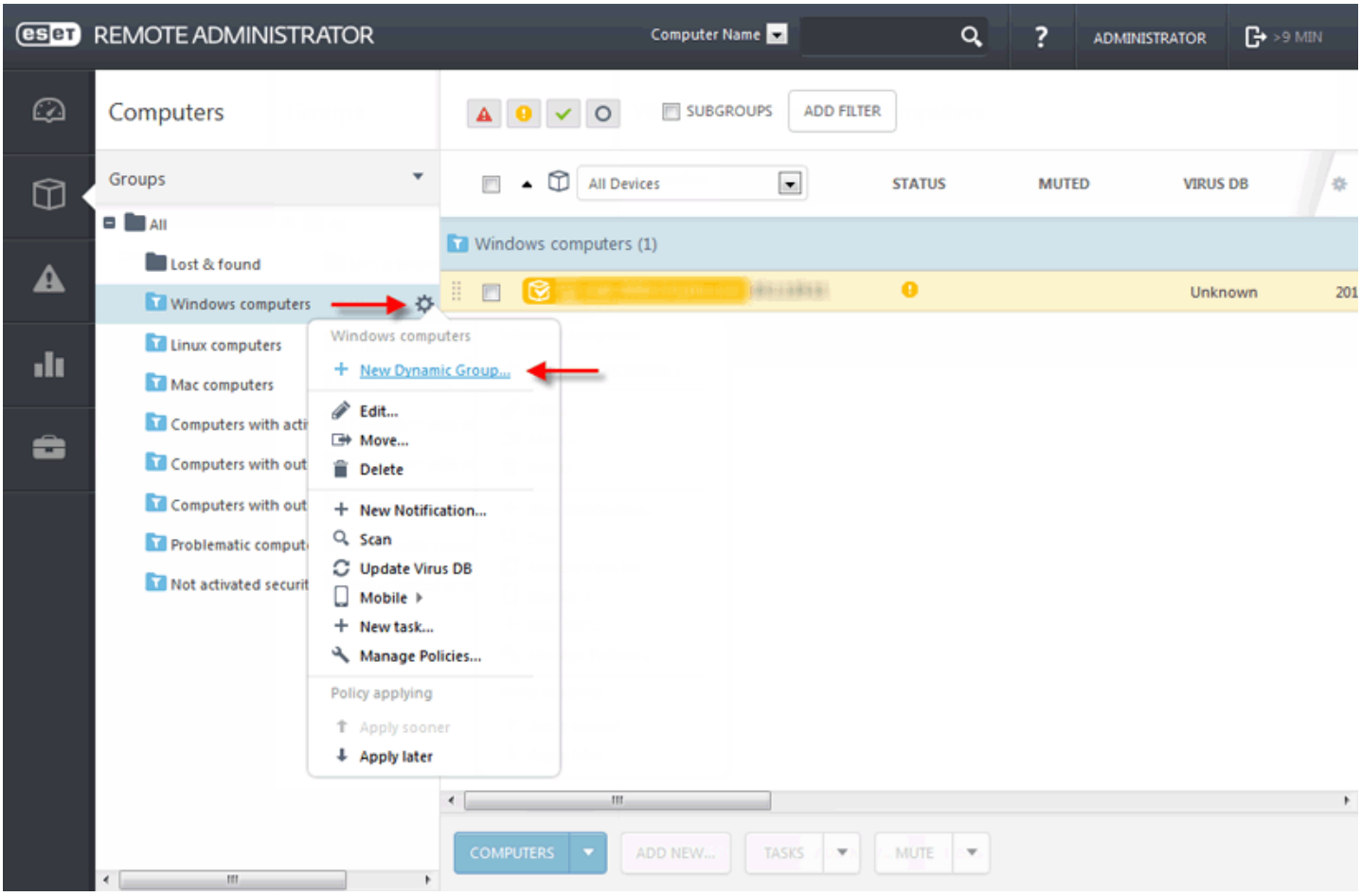
You can either select an existing Dynamic Group template or create a new Dynamic Group template.

Summary

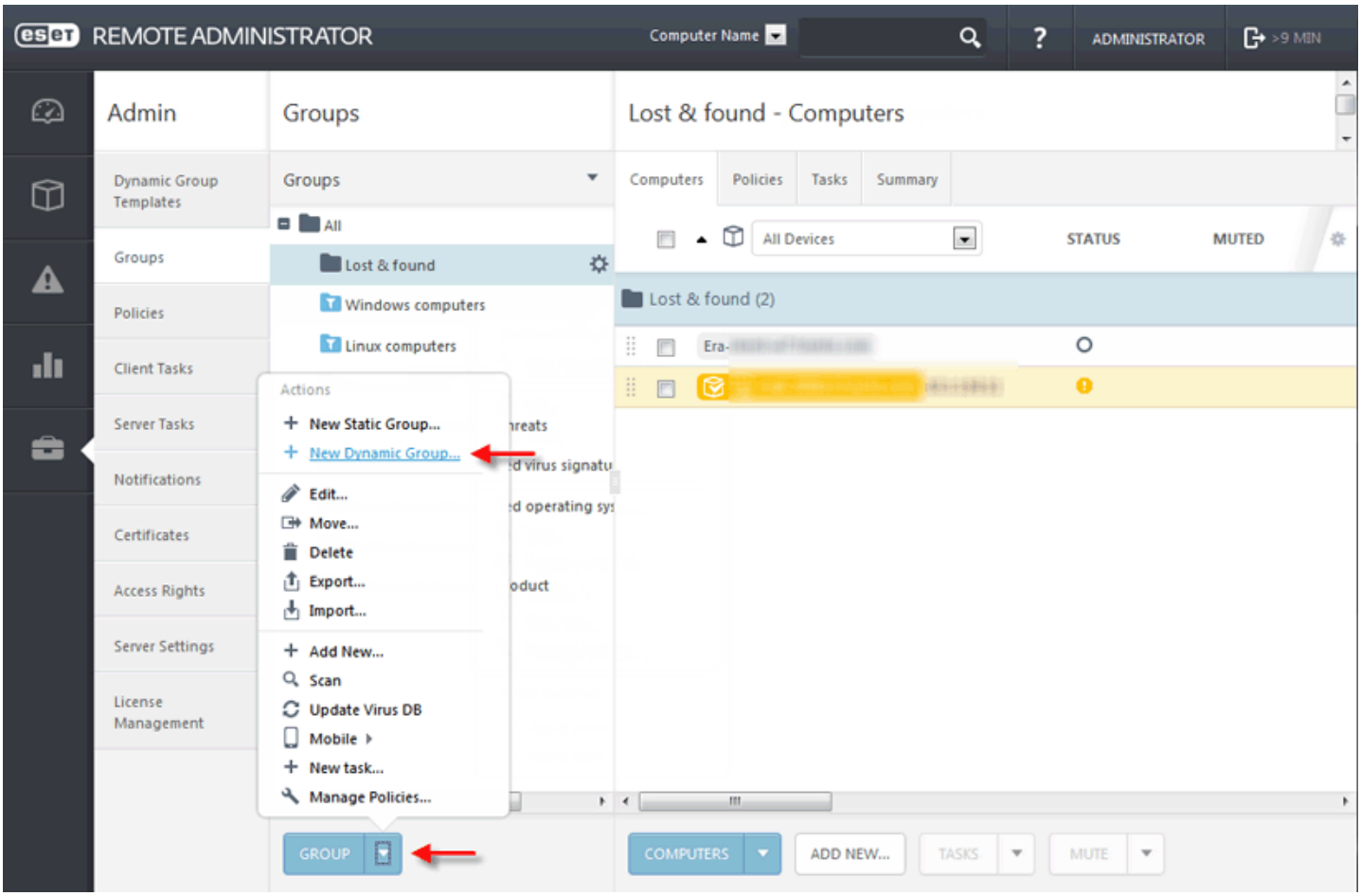
Review the configuration to make sure it is correct (if you need to make changes, you can still do so) and click **Finish**.

6.1.1.7.4 Create Dynamic Group using existing Template

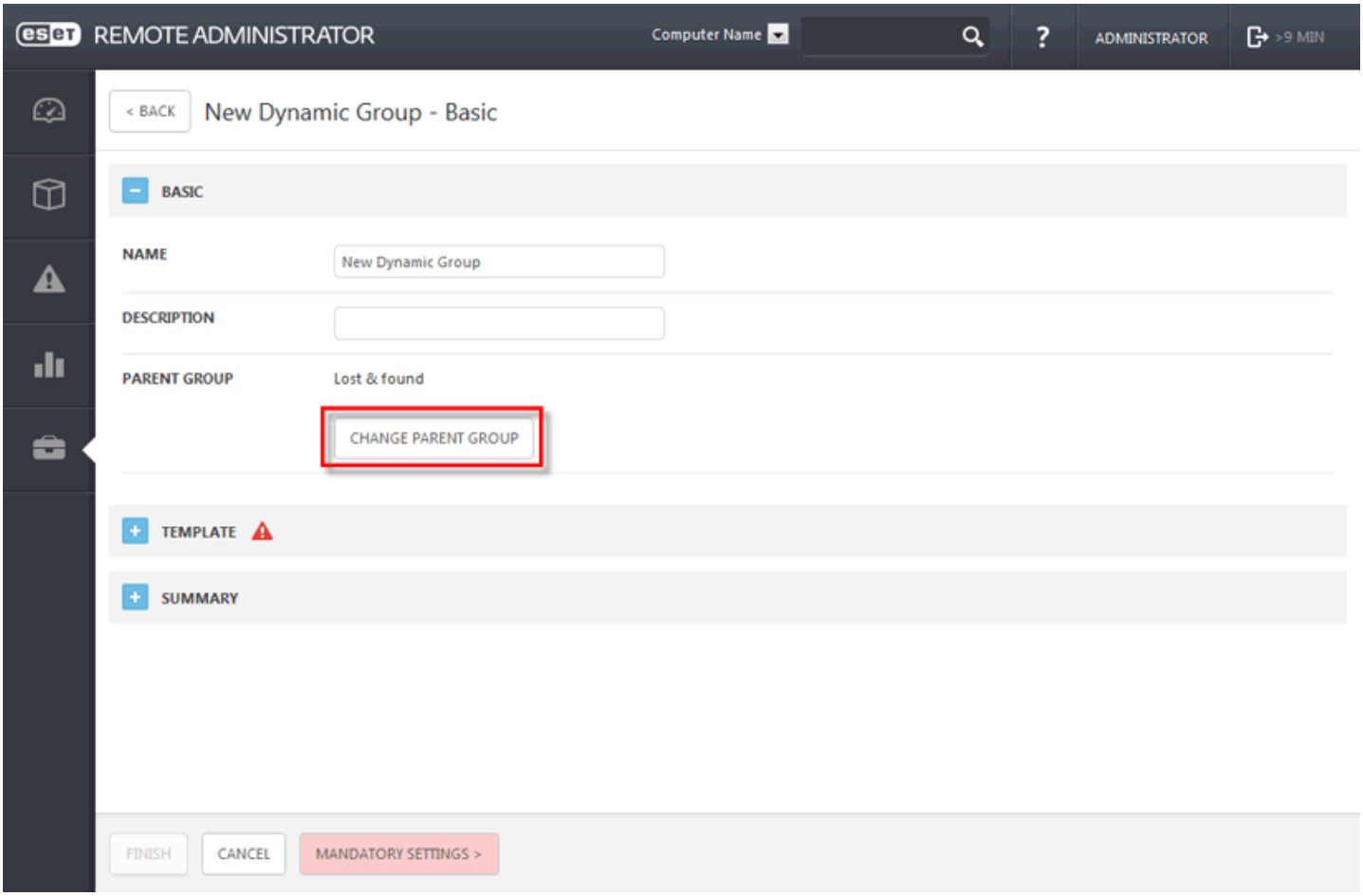
To create a new Dynamic Group using an existing template, click the cogwheel ⚙ next to the Dynamic Group name and then click **New Dynamic Group.**



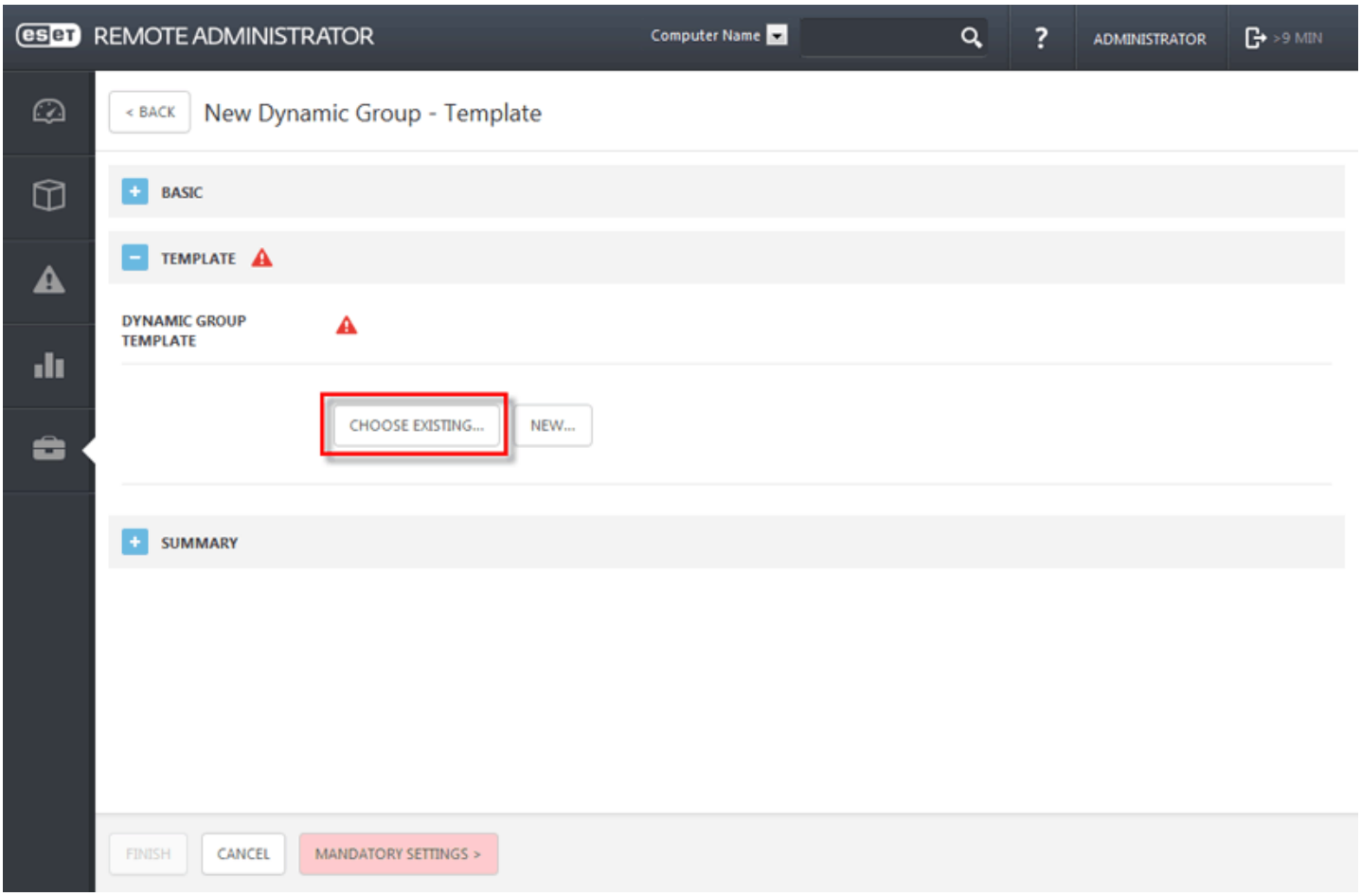
Alternatively, the **New Dynamic Group...** is accessible from **Admin** > **Groups.** Select a group (in the Groups pane) and click **Group** at the bottom.



A Dynamic Group Wizard will appear. Enter a **Name** and **Description** (optional) for the new template. Users can also change the parent group by clicking **Change parent group**.



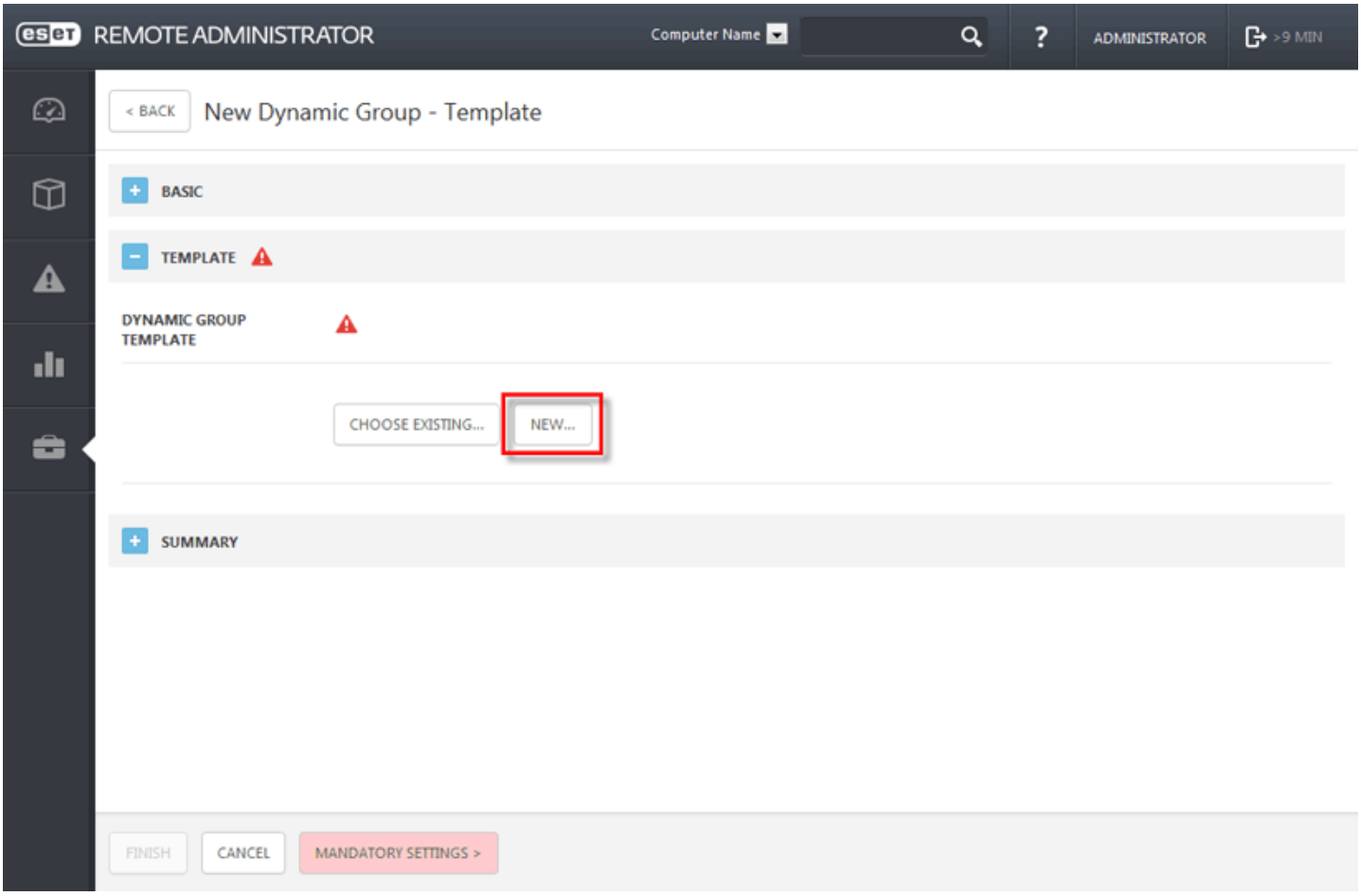
Select **Dynamic Group Template** from the pre-defined templates or select a template you have already created. Click **Choose from existing** and select the appropriate template from the list. If you have not created any templates and none of the pre-defined templates in the list suits you, click **New** and follow the steps to create a new template.



The last screen is a summary. The new group appears under the parent Static Group.

6.1.1.7.5 Create Dynamic Group using new Template

These steps are the same as when creating a Dynamic Group using an existing template up to the **Dynamic Group template** step where you click New Dynamic Group Template and fill-in the details for new template.



Once finished, this new template is automatically used. Also, the template will appear in the Dynamic Group Templates list and can be used to create other Dynamic Groups.

6.1.1.7.6 Manage Dynamic Groups

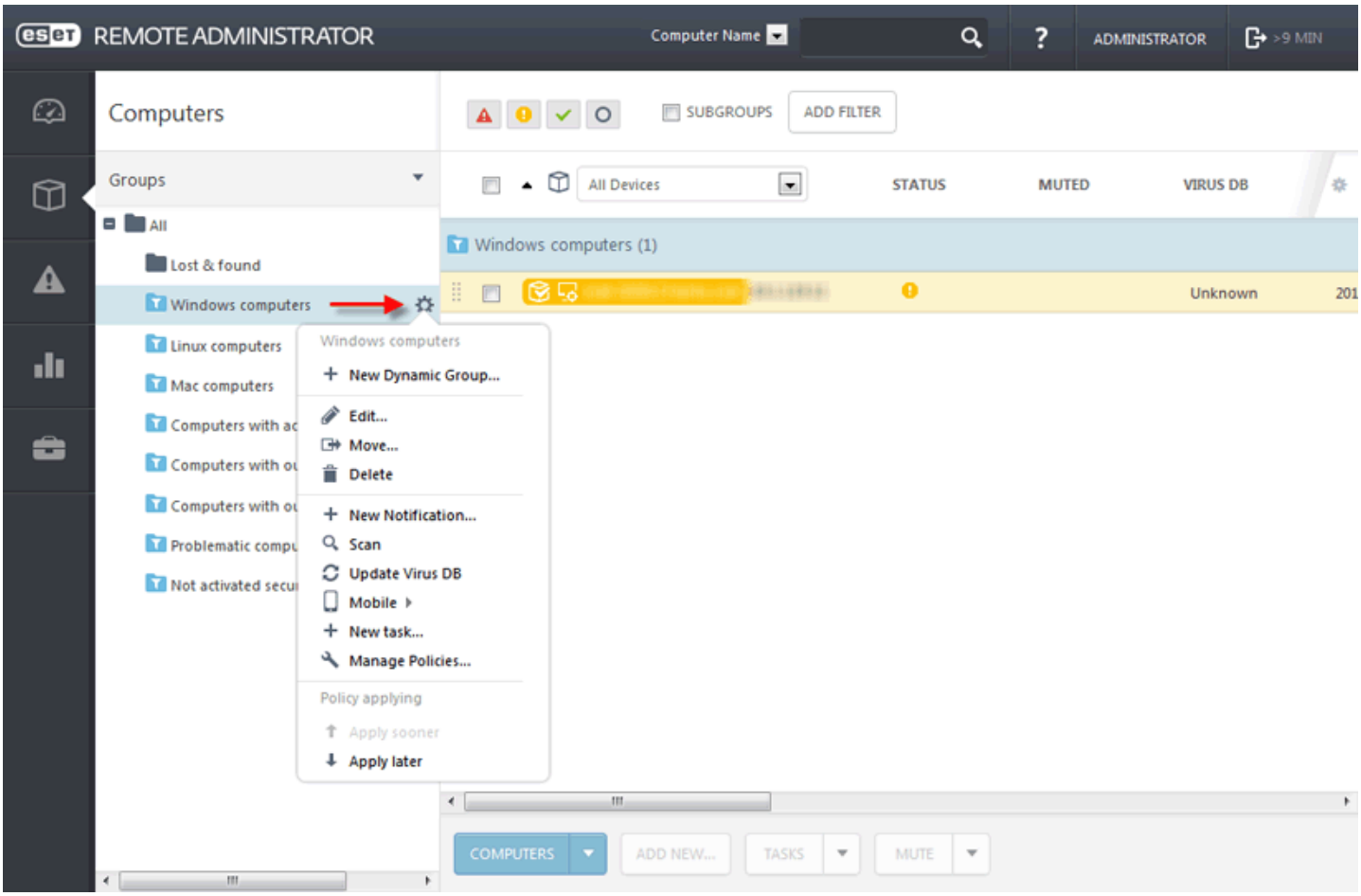
You can create a Dynamic Group using an existing template or create a new template that will be used for this Dynamic Group.

Once created, a user can perform various operations on every Dynamic Group. Operations such as:

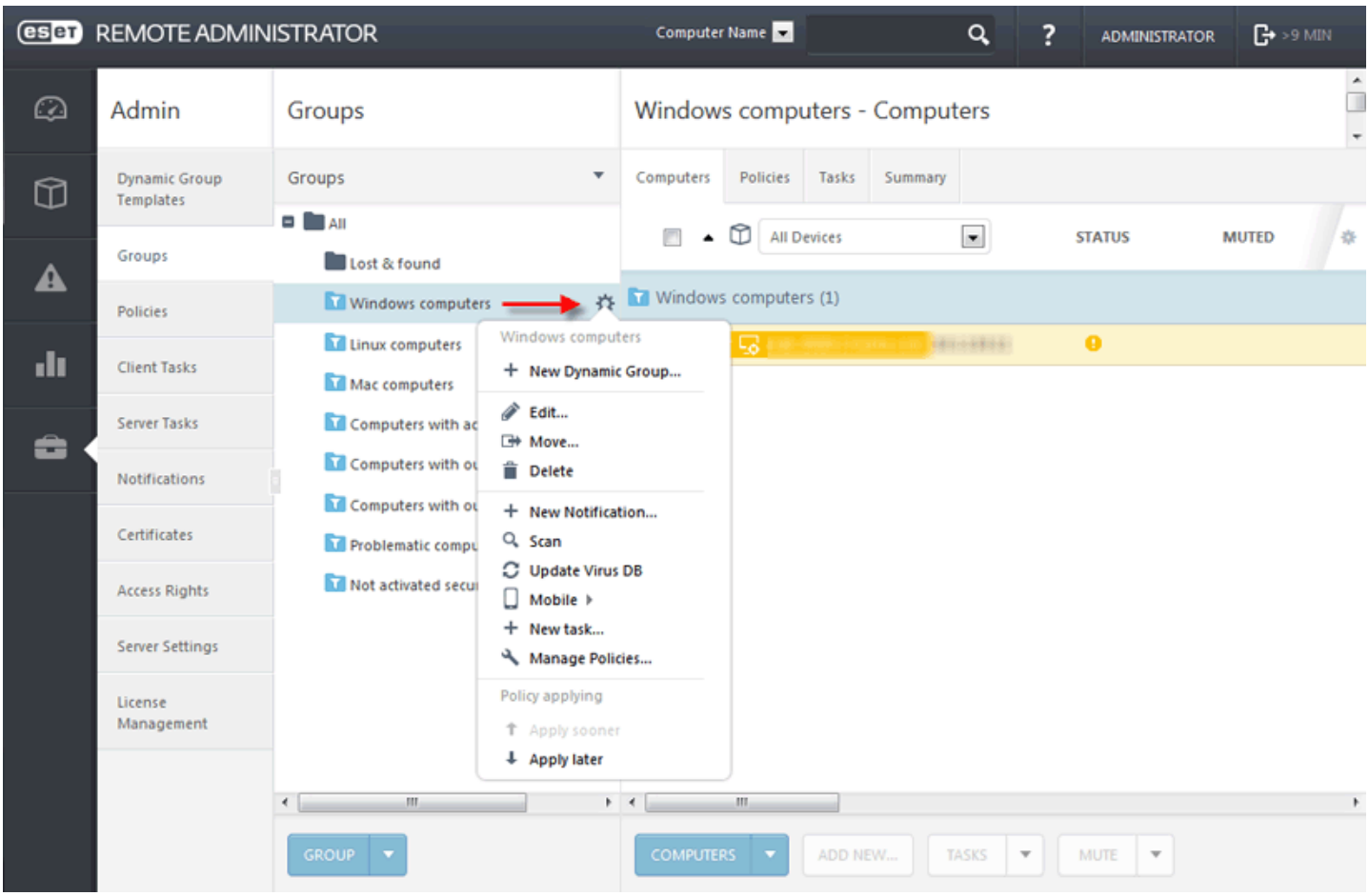
- Edit
- Move
- Delete
- Run Tasks
- Use for Notifications

You can perform these operations from three places:

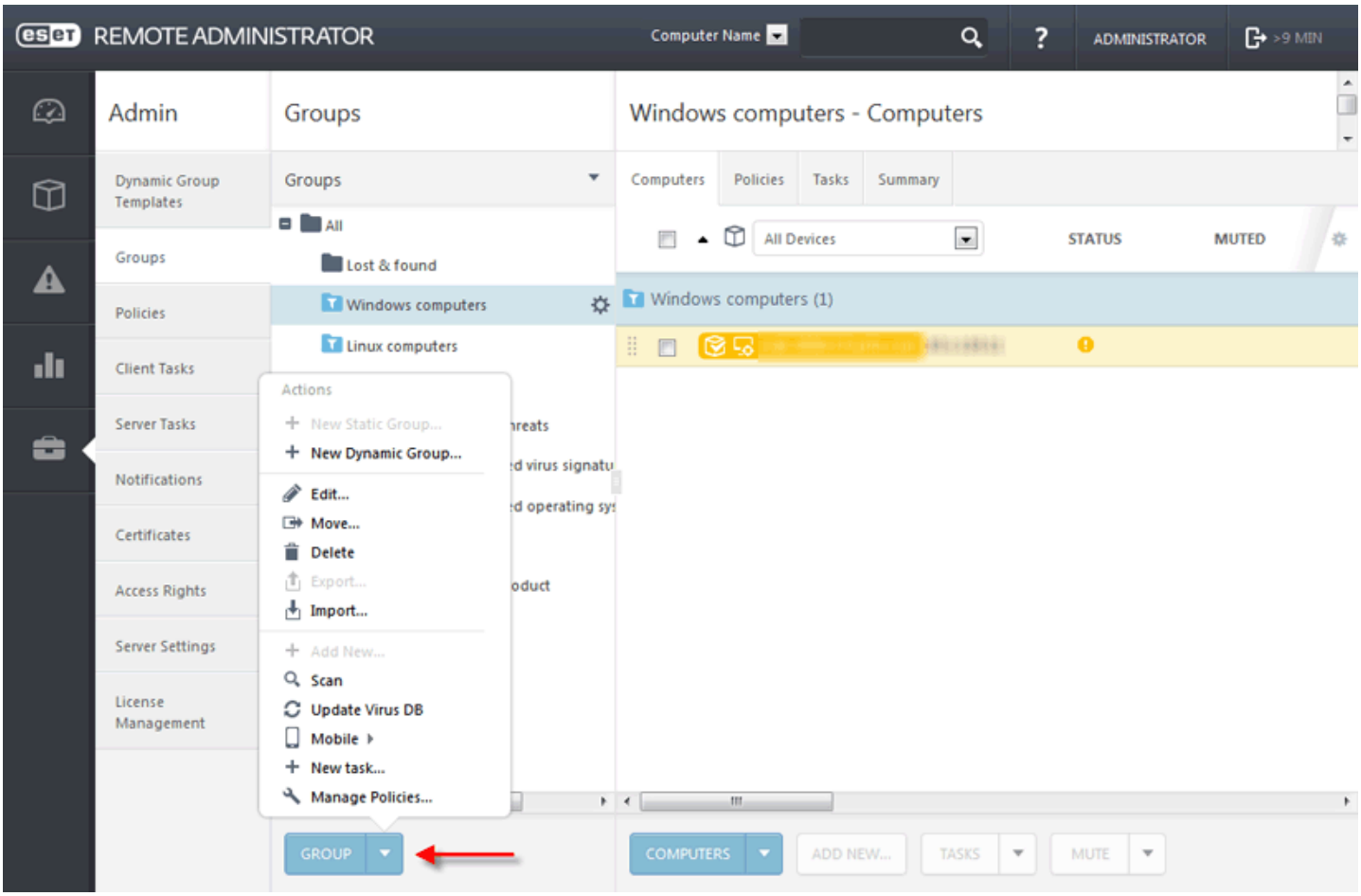
1. **Computer** > **Groups** > ⚙



2. **Admin** > **Groups** > ⚙



3. **Admin** > **Groups** > select Dynamic Groups you want to manage and click **Group**.



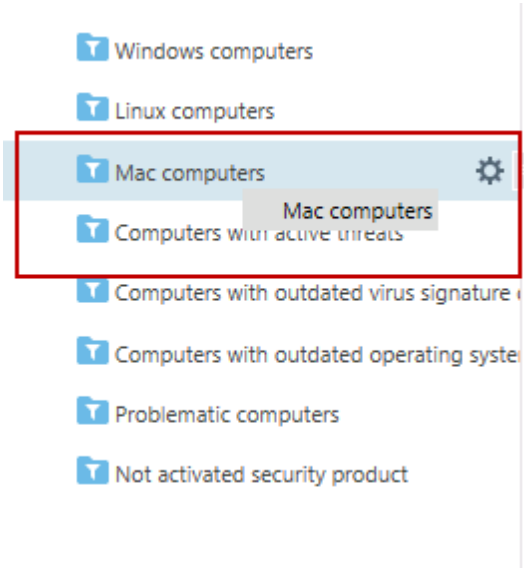
6.1.1.7.7 Move Dynamic Group

Click the cogwheel symbol next to the group name and select **Move**. A pop-up window will be displayed showing the groups tree structure. Select the target group (static or dynamic) into which you want to move the selected group. The target group will become a parent group. You can also move groups by dragging and dropping a group into the target group of your choice.

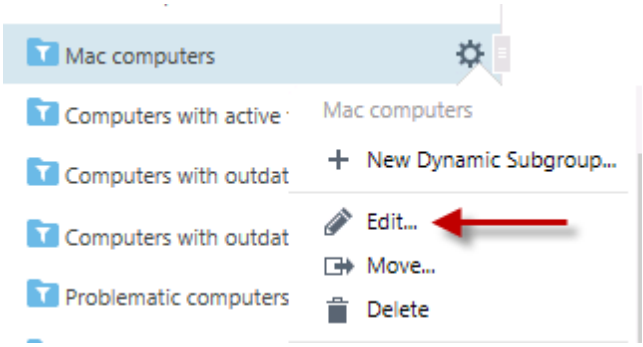
A few exceptions to group organization should be noted. **You cannot move a Static Group into a Dynamic Group**. Also, it is not possible to move pre-defined Static Groups (for example, Lost & found) to any other group. Other groups can be moved freely. A Dynamic Group can be a member of any other group including Static Groups.

The following methods can be used when moving groups:

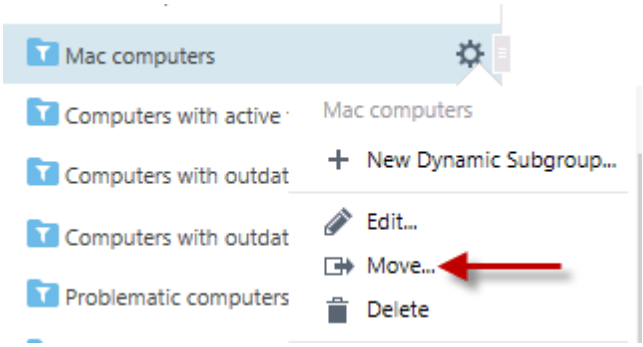
Drag and drop - click and hold the group you want to move and release it above new parent group.



> **Edit** > **Change parent group**.



> **Move** > select a new parent group from the list and click **OK**.



NOTE: The Dynamic Group in a new position starts to filter computers (based on the template) without any relation to its previous location.

6.1.1.7.8 Assign a Policy to a Dynamic Group

Both Static and Dynamic Groups are treated the same way when it comes to policy assignment. For instructions on how to assign a policy to a group, click here.

6.1.1.7.9 Assign a Task to a Dynamic Group

Both Static and Dynamic Groups are treated the same way with regard to task assignment. For instructions on how to assign a task to a group, click here.

6.1.1.7.10 How to automate ESET Remote Administrator

1. Create a Dynamic Group for example: "Infected Computers"
2. Create a task, for in-depth scan and assign that to dynamic group Infected Computers (Task triggered when clients enters Dynamic Group)
3. Create a specific policy (in this case "isolation policy") - when an ESET security product is installed, create a Firewall rule that will block all traffic, except the connection to ESET Remote Administrator.
4. Create a notification template for infected computers (you can specify various conditions) a notification is triggered to alert you of a spreading threat.

- Using the same technique, you can automate product and OS updates, scanning, automatic activations of newly added products with a pre-selected license, and other tasks.

6.1.1.7.11 When does a computer become a member of a Dynamic Group?

For a computer to become a member of particular Dynamic Group, it needs to meet certain conditions. These conditions are defined in a Dynamic Group Template. Each template consists of one or several Rules (=Conditions). You can specify these rules when creating a new Template.

Certain information about current condition of a client computer is stored at the Agent. Then the computer's condition is being evaluated by the Agent according to the Template rules.

ERA user may only be interested in certain status(es). He/she defines such a state by specifying values for particular statuses – this pre-defined set is called Dynamic Group.

As soon as any machine enters into state of these specific values, it is automatically assigned to this group.

Dynamic Groups can be seen as filters based on computer status. One computer may apply for more than one filters and, therefore, be assigned to more than one Dynamic Group. This makes Dynamic Groups different from Static Groups, in which a computer can reside once only.

6.1.1.7.12 Template Rules Evaluation

Template rules evaluation is handled by the Agent, not the ERA Server (only the result is sent to the ERA Server).The evaluation process is happens according to the rules that are configures in a Template. The following is an explanation of the evaluation process with a few examples.

Status is a cluster of various information. Some sources provide more than one dimensional status per machine (for example, Operating System, RAM size, etc.), others provide multidimensional status information (for example, IP Address, Installed Application, etc).

Below is a visual representation of the status of a client:

Network Adapters - IP Address	Network Adapters - MAC Address	OS Name	OS Version	HW - RAM size in MB	Installed Application
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Status is made of information groups. One group of data always provides coherent information organized into rows. The number of rows per group may vary.

Conditions are evaluated per group and per row - if there are more conditions regarding the columns from one group, only the values on the same row are considered.

Example 1:

For this example consider the following condition:

```
Network Adapters.IP Address = 10.1.1.11 AND Network Adapters.MAC Address = 4A-64-3F-10-FC-75
```

This rule matches no computer, as there is no such row where both conditions hold true.

Network Adapters - IP Address	Network Adapters - MAC Address	OS Name	OS Version	HW - RAM size in MB	Installed Application
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Example 2:

For this example consider the following condition:

```
Network Adapters.IP Address = 192.168.1.2 AND Network Adapters.MAC Address = 4A-64-3F-10-FC-75
```

This time, both conditions matched cells on the same row and therefore, the rule as a whole is evaluated to TRUE. A computer is selected.

Network Adapters - IP Address	Network Adapters - MAC Address	OS Name	OS Version	HW - RAM size in MB	Installed Application
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Example 3:

For conditions with the OR operator (at least one condition must be TRUE), such as:

```
Network Adapters.IP Address = 10.1.1.11 OR Network Adapters.MAC Address = 4A-64-3F-10-FC-75
```

the rule is TRUE for two rows, as only either of the conditions must be satisfied. A computer is selected.

Network Adapters - IP Address	Network Adapters - MAC Address	OS Name	OS Version	HW - RAM size in MB	Installed Application
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

6.1.1.7.13 Rule Editor

Conditions

When you set conditions for a Dynamic Group template, there are different operators used for different conditions.

There are 3 types of lists:

- Numeric operator lists contain operators that compare numeric values
- String operator lists contain operator that compare alphanumeric values
- Boolean operator lists contain only two operators, true "= (equal)" and false "≠ (not equal)"

Operators Lists types

The list contains 6 values:

- "= (equal)"
- "≠ (not equal)"
- "> (greater than)"
- "≥ (greater or equal)"
- "< (less than)"
- "≤ (less or equal)"

String operators list

The list contains 9 values:

- "= (equal)" - set only exact and whole searched value
- "≠ (not equal)" - set only exact and whole value that you want search to ignore
- "has substring" - set substring anywhere in the expression
- "has prefix" - set exactly few first characters from searched string, e. g. string "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", the prefix means "Micros" or "Micr" or "Microsof"etc.
- "has postfix" - set exactly few last characters from searched string, e. g. string "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", the postfix means "319" or "0.30319", etc.
- "regex" - uses a Perl syntax
- "in" - set exact expression, e. g. string "Microsoft Windows" you have to write exactly "Microsoft Windows"
- "has mask" and "in (string mask)"have 2 kinds of wildcard characters:
- * - matching any number of characters (0 or more)
- ? - matching exactly 1 character

Examples

- "a*" matches "a", "aa", "ax", "abcde"
- "a?" matches "aa", "ab", "ac", but not "a" or "aaa"
- "a??" marches "aaa", "aab", "axy", but not "a", "aa" or "aaaa"
- "a?*" matches "aa", "ax", "abcde", but not "a"
- "*a*" matches "a", "xa", "ax", "xax", "dynamic", "abba"
- "?*" matches anything except ""

Boolean operators list

The list contains 2 values, but these values are always connected to second condition's list:

- "= (equal)" - next condition is true
- "≠ (not equal)" - next condition is false

- The basic mathematical operations (e.g. greater than) are pretty self-explaining. For the others, providing a short explanation:

has substring" operator. True if the operand is a substring of the symbol value.
"has prefix" operator. True if the symbol value starts with the value of the operand. E.g. "xyz" has prefix "xy".
"has postfix" operator. True if the symbol value ends with the value of the operand. E.g. "xyz" has postfix "yz".
"has mask" operator. Allows the use of wildcards for string comparison. E.g. "*z" matches "xyz"
"regex" operator. True if the symbol matches the regex in the operand. Perl regex syntax is used.
"in" operator. The operand is a list of values. True if the symbol value equals to at least one of the operand values. E.g. "xyz" in ("abc", "def", "xyz").
"in (string mask)" operator. The operand is a list of values which allow wildcards. True if the symbol value matches at least one of the operand values. E.g. "xyz" in ("a*", "*f", "*z").
"has no value" operator. True if the symbol has no value. Second operand is ignored.
"has value" operator. True if the symbol has a value. Second operand is ignored.

6.1.2 Policies

Policies are used to push specific configurations to ESET products running on client computers. This allows you to avoid configuring each client's ESET product manually. A policy can be applied directly to individual Computers as well as groups (Static and Dynamic). You can also assign multiple policies to a computer or a group, unlike in ESET Remote Administrator 5 and earlier where it was only possible to apply one policy to one product or component.

Policy application

Policies are applied in the order that Static Groups are arranged. This is not true for Dynamic Groups, where child Dynamic Groups are traversed first. This allows you to apply policies with greater impact at the top of the Group tree and apply more specific policies for subgroups. With properly configured policies with flags, an ERA user with access to groups located higher in the tree can override the policies of lower Groups. The algorithm is explained details in How Policies are applied to clients.

Merging policies

A policy applied to a client is usually a result of multiple policies being merged into one final policy.

NOTE: We recommend that you assign more generic policies (for example, general settings such as update server) to groups that are higher within the groups tree. More specific policies (for example device control settings) should be assigned deeper in the groups tree. The lower policy usually overrides the settings of the upper policies when merging (unless defined otherwise with policy flags).

NOTE: When you have a policy in place and decide to remove it later on, the configuration of the client computers will not automatically revert back to their original settings once the policy is removed. The configuration will remain according to the last policy that was applied to the clients. The same thing happens when a computer becomes a member of a Dynamic Group to which a certain policy is applied that changes the computer's settings. These settings remain even if the computer leaves the Dynamic group. Therefore, we recommend that you create a policy with default settings and assign it to the root group (**All**) to have the settings revert to defaults in such a situation. This way, when a computer leaves a Dynamic group that changed its settings, this computer receives the default settings.

6.1.2.1 Policies Wizard

You can use policies to configure your ESET product the same way you would from within the Advanced setup window of the product GUI. Unlike policies in Active Directory, ERA Policies cannot carry any script or series of commands.

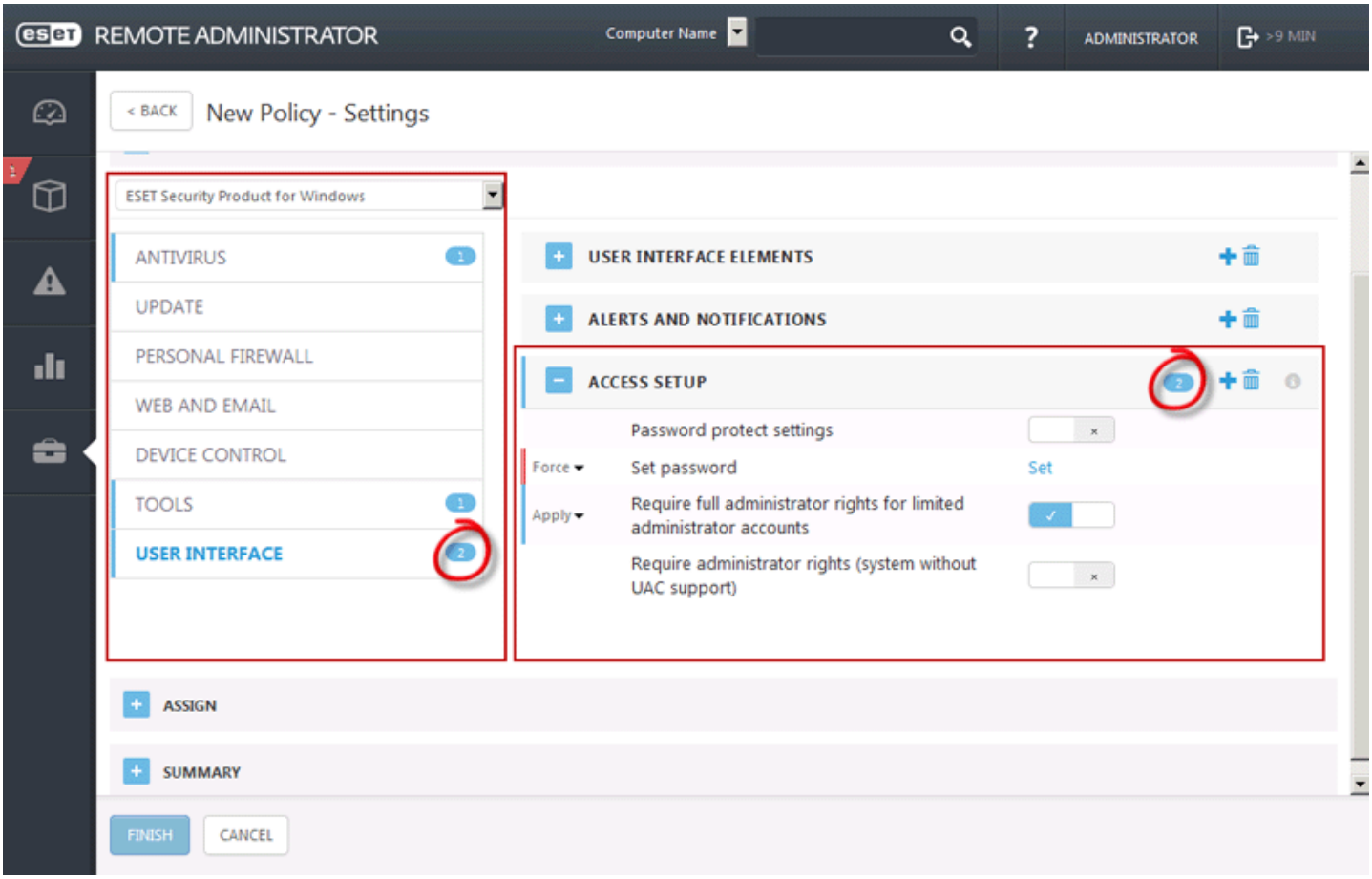
Policies are created and managed in the **Admin** > **Policies** tab. Click **Policies** at the bottom and select New from the context menu.

Basic

Enter a **Name** for the new policy. The **Description** field is optional.

Settings

Select your product from the drop-down menu.



Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a flag. To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to a category name in the tree on the left. This shows a sum of rules in all its sections. This way, you'll quickly see where and how many settings/rules are defined.

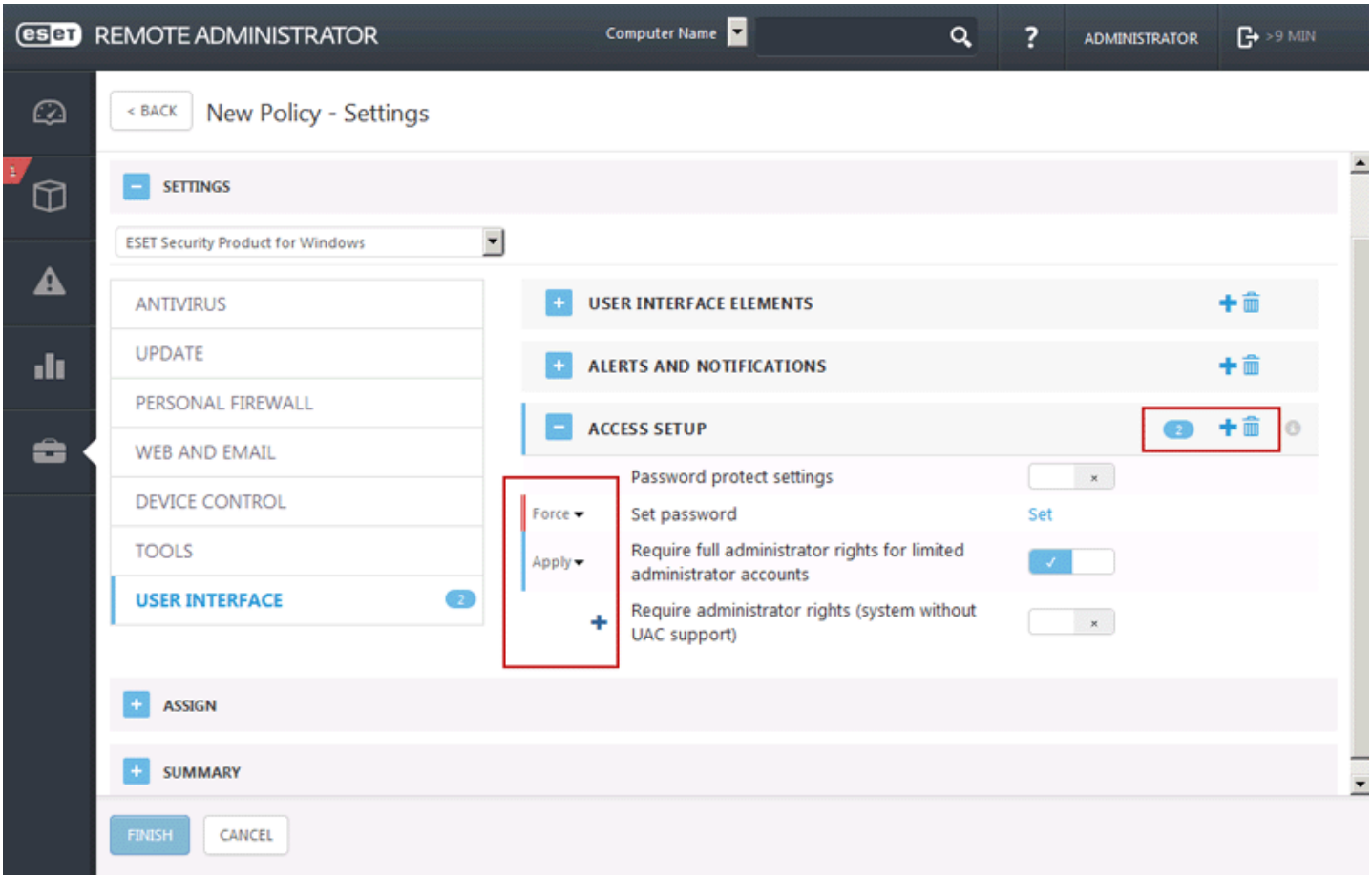
You can also use these suggestions to make policy editing easier:

- use + to set **Apply** flag to all item in current a section
- delete rules using **Trashcan** icon

6.1.2.2 Flags

You can set a flag for each setting in a policy. They define how a setting will be handled by the policy:

- **Apply** - settings with this flag will be sent to the client. However, when merging policies it can be overwritten by a later policy. When a policy is applied to a client computer and a particular setting has this flag, that setting is changed regardless of what was configured locally on the client. Because the setting is not forced, it can be changed by other policies later on.
- **Force** - settings with the force flag have priority and cannot be overwritten by a later policy (even if the later policy has a Force flag). This assures that this setting won't be changed by later policies during merging.



Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a flag. To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to a category name in the tree on the left. This shows a sum of rules in all its sections. This way, you'll quickly see where and how many settings/rules are defined.

You can also use these suggestions to make policy editing easier:

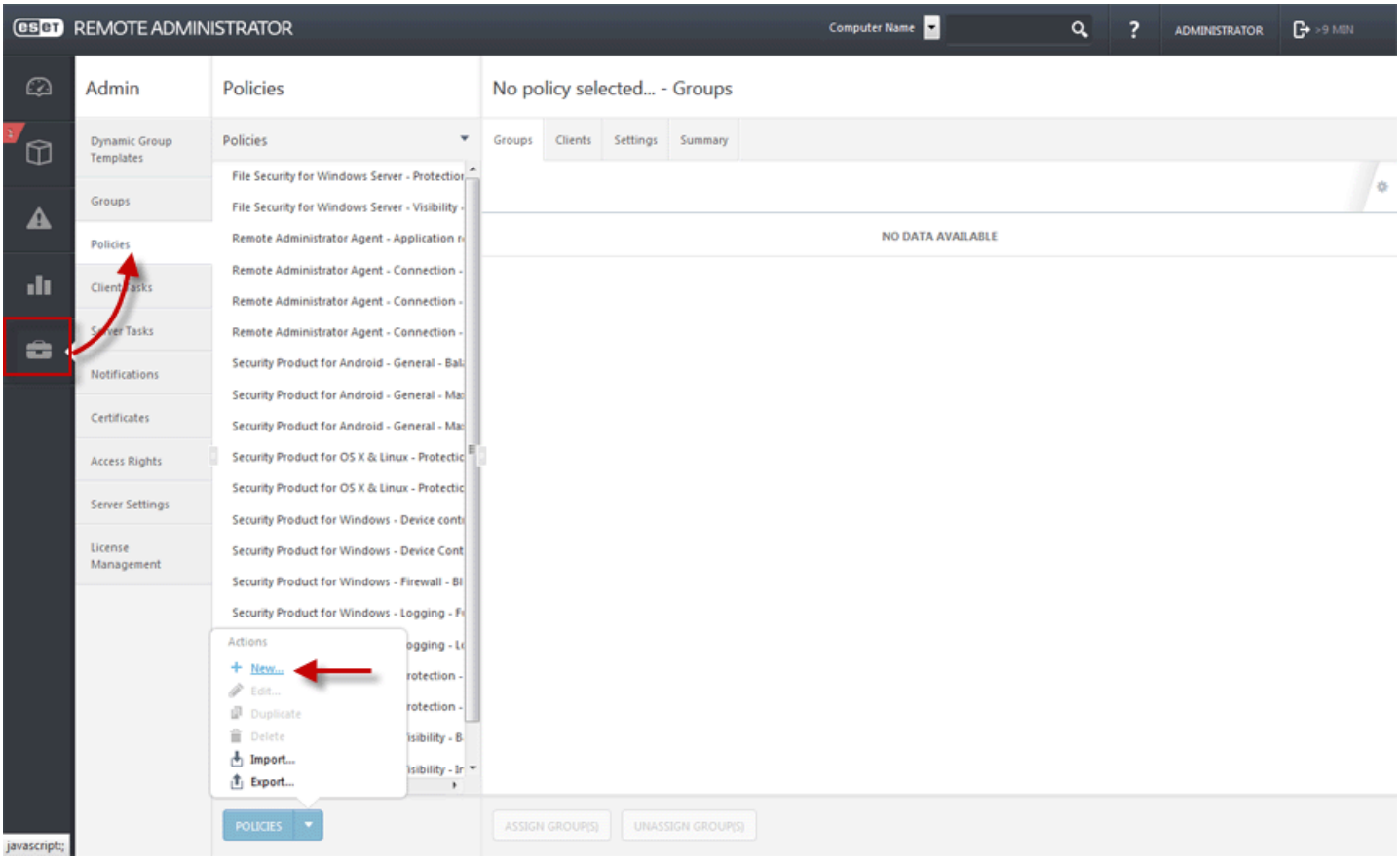
- use + to set **Apply** flag to all item in current a section
- delete rules using **Trashcan** icon

6.1.2.3 Manage Policies

In this example, we are going to create a new policy for the ERA Agent Connection Interval. We highly recommend doing this prior to testing mass deployment in your environment.

1. Create a New Static Group.

2. Add a new policy by clicking **Admin** > **Policies**. Click **Policies** at the bottom and select **New**.

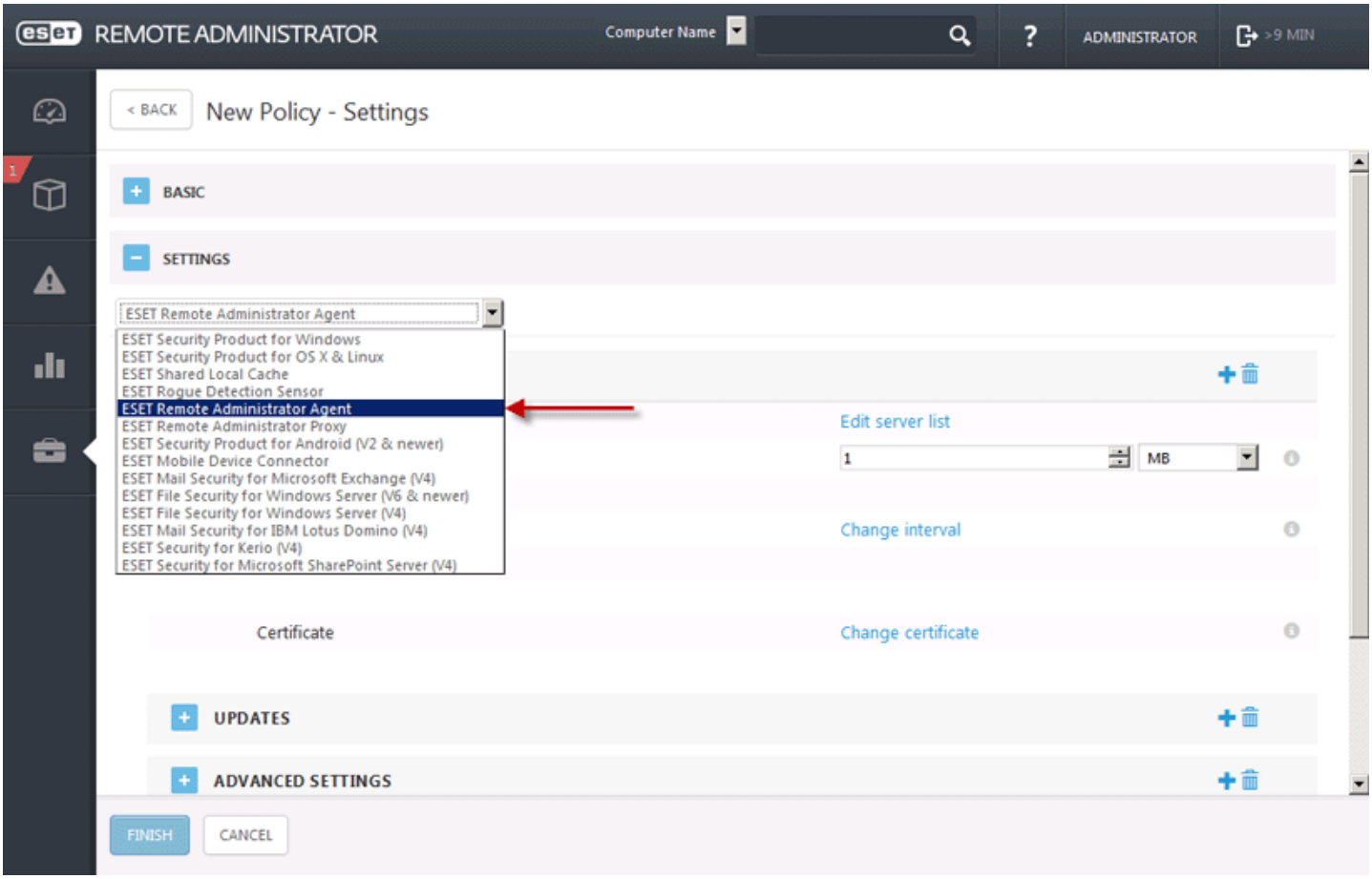


Basic

Enter a **Name** for the new policy (for example "Agent Connection Interval"). The **Description** field is optional.

Settings

Select **ESET Remote Administrator Agent** from the **Product** drop-down menu.



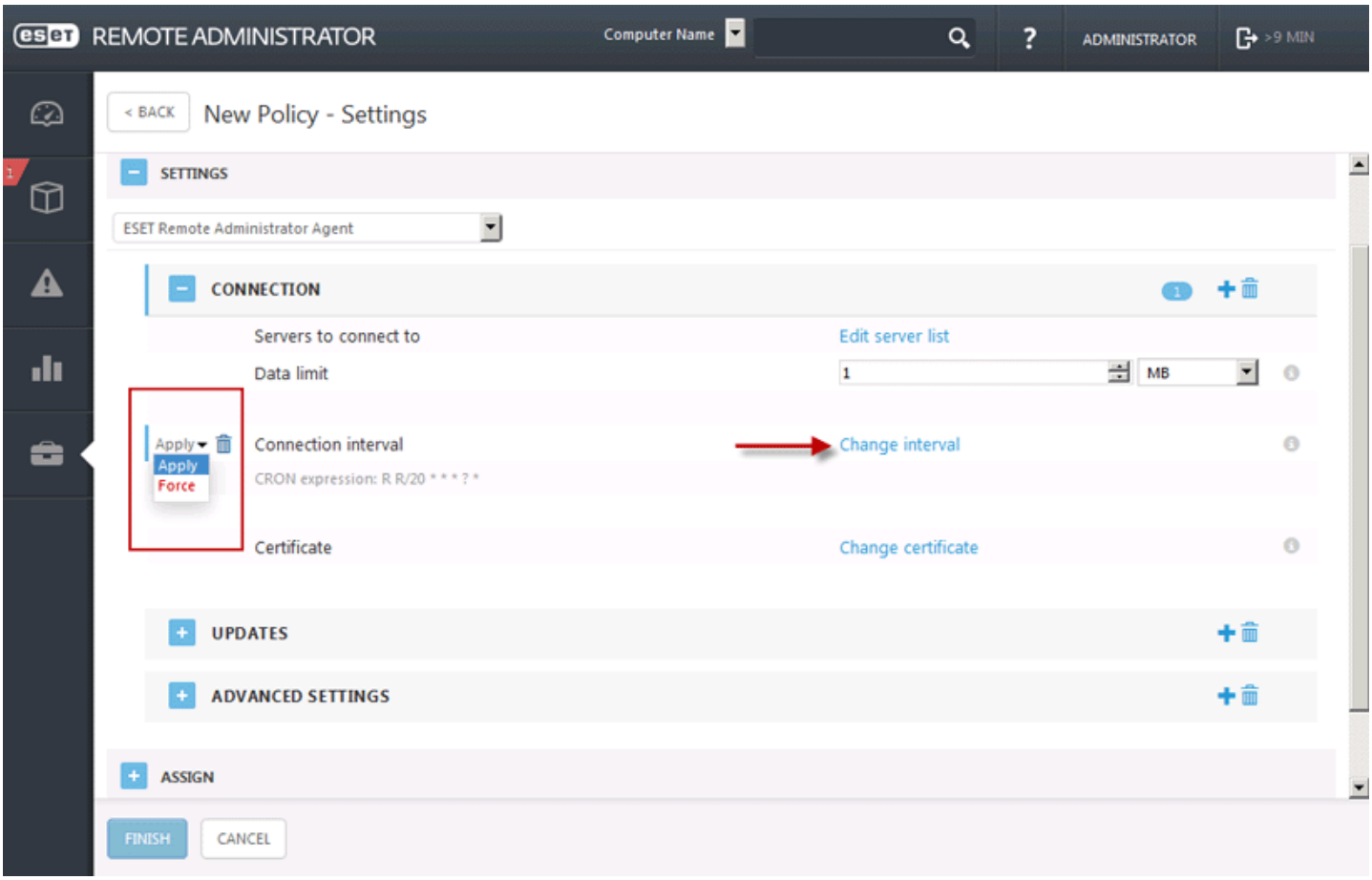
Connection

Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a flag. To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to a category name in the tree on the left. This shows a sum of rules in all its sections. This way, you'll quickly see where and how many settings/rules are defined.

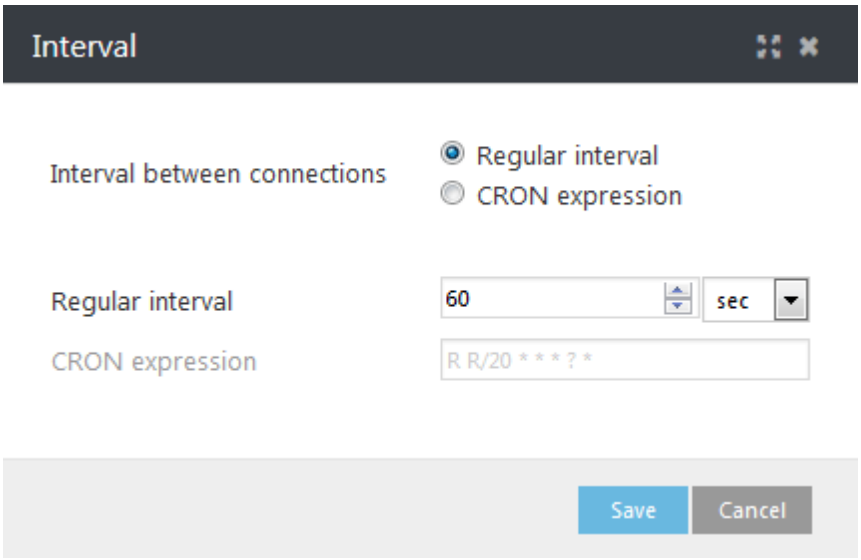
You can also use these suggestions to make policy editing easier:

- use + to set **Apply** flag to all item in current a section
- delete rules using **Trashcan** icon

Click **Change interval**.



In the **Regular interval** field, change the value to your preferred interval time (we recommend 60 seconds) and click **Save**.



Once you've created a new Agent Connection Interval policy, assign it to the Static Group you created in step 1.

After you are finished with mass deployment testing, edit the ERA Agent Connection Interval policy settings you created in step 2.

Click **Admin** > **Groups** and select the **Policies** tab. Click **Agent Connection Interval policy**, choose **Edit** and then click **Settings** > **Connection**. Click **Change Interval** and set the connection interval to 20 minutes.

6.1.2.4 How Policies are applied to clients

Groups and Computers can have several policies assigned to them. Moreover, a Computer can be in a deeply nested Group, the parents of which have their own policies.

The most important thing for the application of policies is their order. This is derived from the Group order and order of policies assigned to the Group.

Follow the steps below to determine the active policy for any client:

1. Find the order of groups in which the client resides
2. Replace groups with assigned Policies
3. Merge Policies to get final settings

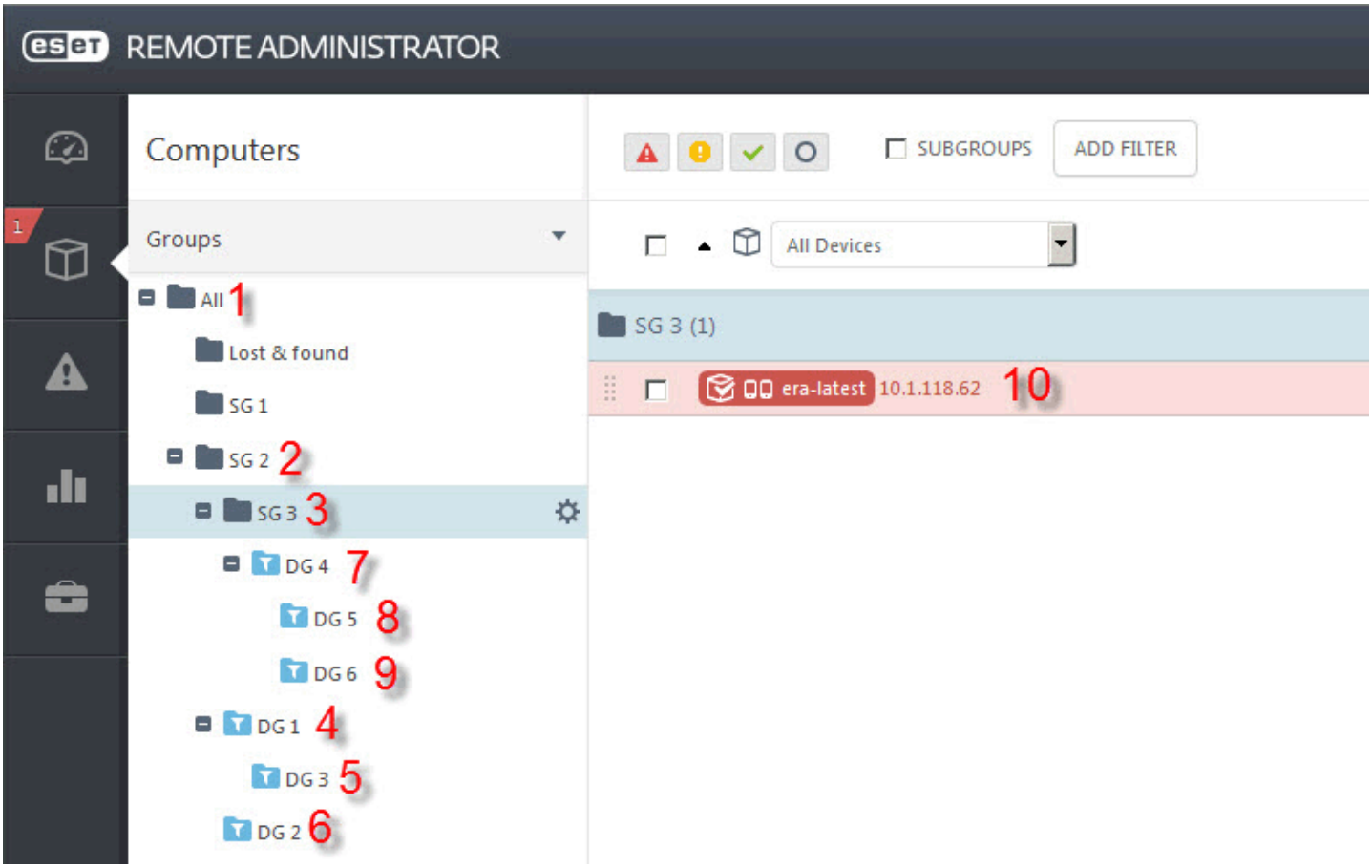
6.1.2.4.1 Ordering Groups

Policies can be assigned to **Groups**, and are applied in a specific order.

When ordering Groups into the list, several rules are applied:

1. Static Groups are traversed from the root Static Group - All.
2. On every level, the Static Groups of that level are traversed first in the order they appear in the tree - this is also called Breadth-first search.
3. After all the Static Groups at a certain level are in the list, Dynamic Groups are traversed.
4. In every Dynamic Group, all its children are traversed in the order that they appear in the list.
5. At any level of Dynamic Groups, if there is a child, it is listed and searched for its children. When there are no more children, the next Dynamic Groups at the parent level are listed - this is also called Depth-first search.
6. Traversal ends at a Computer.

In practice, the traversal would look as follows:



As shown above, the root (Static Group called **All**) is listed as **Rule 1**. Since there are no more groups at the same level as the **All** group, policies from groups at the next level are evaluated next.

The **Lost & Found**, **SG 1** and **SG 2** Static Groups are evaluated next. The computer is actually only a member of the **All/SG 2/SG 3** Static Groups and therefore there is no need to traverse the **Lost & Found** and **SG 1** groups. **SG 2** is the only group at this level that will be evaluated, so it goes into the list and traversal goes deeper.

At the third level, the algorithm finds **SG 3**, **DG 1** and **DG 2**. According to **Rule 2**, Static Groups are listed first. Traversal adds **SG 3** and, since it is the last Static Group at level 3, moves to **DG 1**. Before moving on to **DG 2** at level 3, the children of **DG 1** must be listed.

DG 3 is added. It has no children, so traversal steps up.

DG 2 is listed. It has no children. At level 3, there are no more groups left. Traversal steps to level 4.

Only Dynamic Group **DG 4** and the computer itself are on level 4. **Rule 6** says that the computer goes last, hence **DG 4** is picked up. **DG 4** has two children that must be processed before going any further.

DG 5 and **DG6** are added to the list. They both lack children and traversal has nothing more to process. It adds **Computer** and ends.

We ended up with the list:

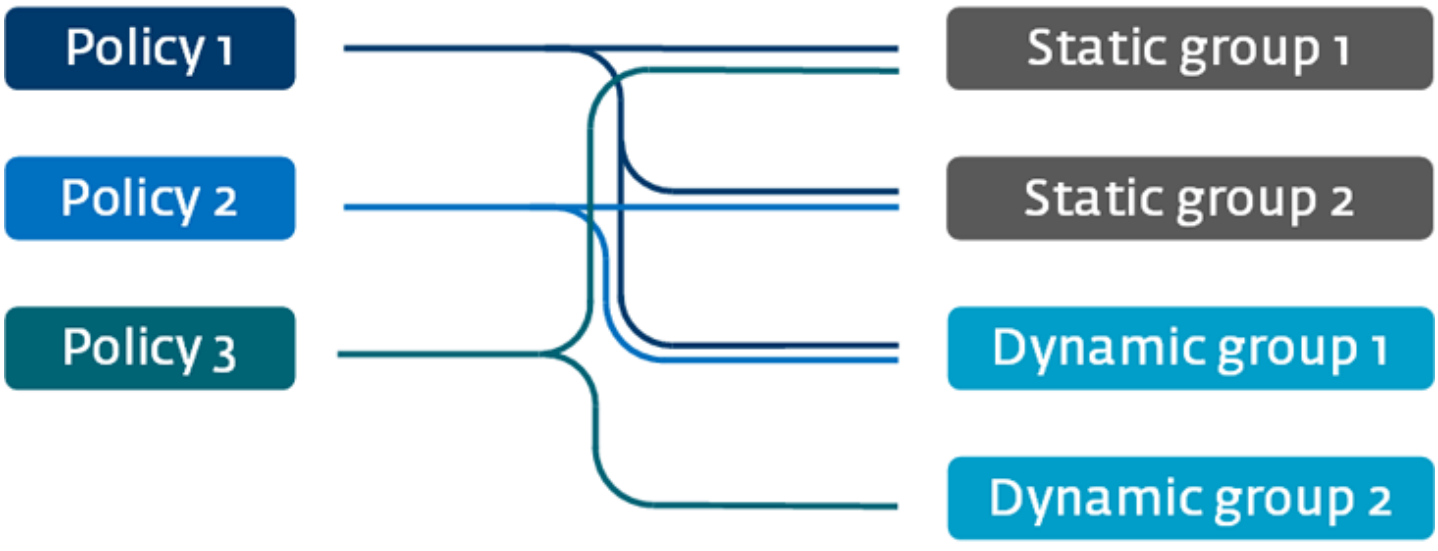
1. All
2. SG 2
3. SG 3
4. DG 1
5. DG 3
6. DG 2
7. DG 4
8. DG 5
9. DG 6
10. Computer

This is the order in which the Policies are applied.

6.1.2.4.2 Enumerating Policies

Once the order of Groups is known, the next step is to replace each group with the policies assigned to it. Policies are listed in the same order as they are assigned to a Group. A group without a policy is removed from the list. It is possible to edit the priority of policies for a group with more policies assigned. Each policy configures only one product (ERA Agent, ERA Proxy, EES, etc.)

We have 3 policies applied to both static and Dynamic Groups (see picture below):



Our list from step 1 would be transformed into:

1. All (removed, no Policy here)
2. SG 2 -> Policy 1, Policy 2
3. SG 3 (removed for no Policy)
4. DG 1 -> Policy 1, Policy 2
5. DG 3 (removed, no Policy)
6. DG 2 -> Policy 3
7. DG 4 (removed, no Policy)
8. DG 5 (removed, no Policy)
9. DG 6 (removed, no Policy)
10. Computer (removed, no Policy)

The final list of Policies is:

1. Policy 1
2. Policy 2
3. Policy 1
4. Policy 2
5. Policy 3

6.1.2.4.3 Merging Policies

Policies are merged one by one. When merging policies, the general rule is that the latter policy always replaces the settings set by the former one.
To change this behavior, you can use policy flags (available for every setting). Settings are merged one by one.

Keep in mind that the structure of the groups (their hierarchy) and the sequence of the policies determines how the policies are merged. Merging of any two policies may have different result in dependence on their order. The groups have been ordered and policies have been enumerated.

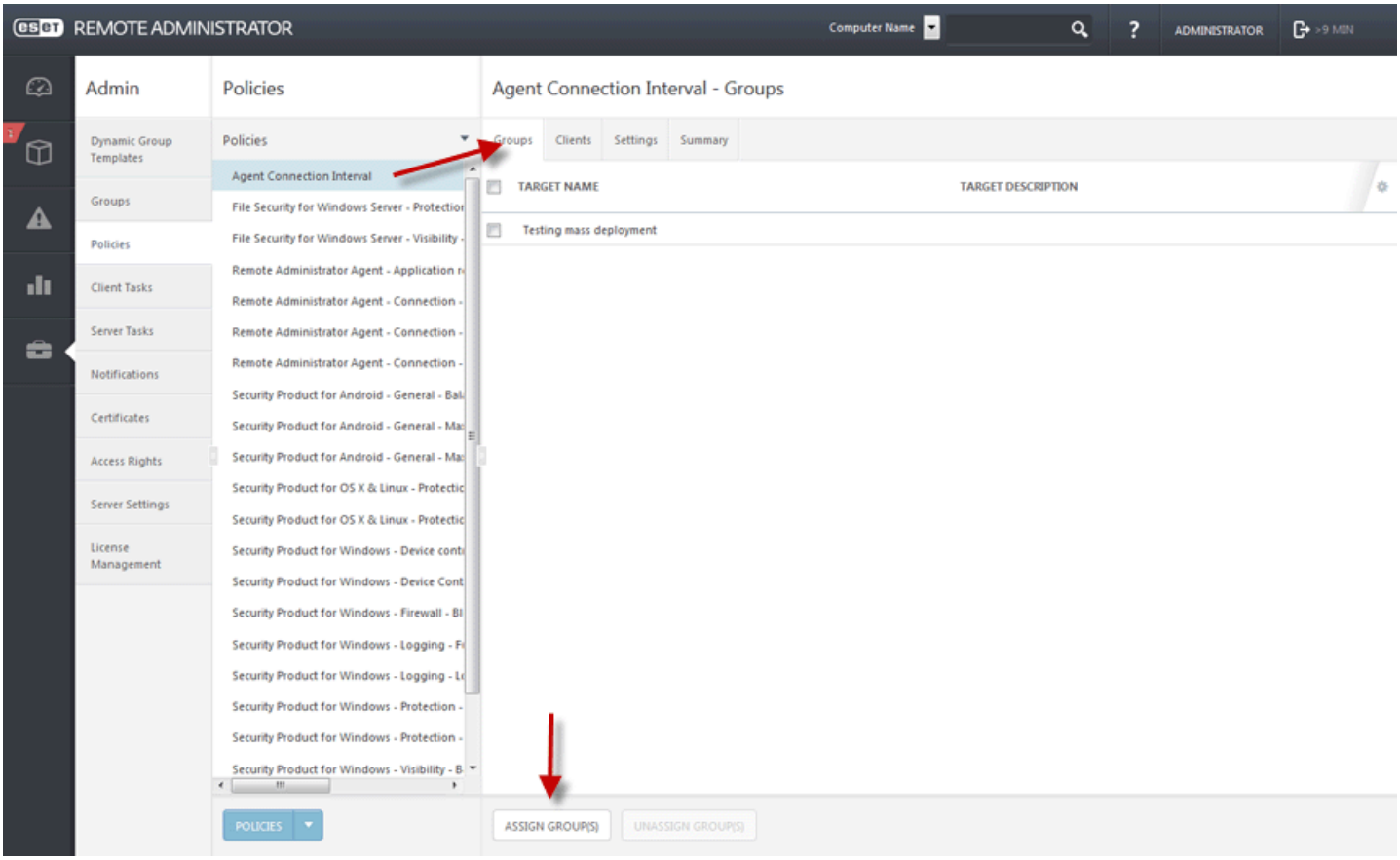
6.1.2.5 Configuration a product from ERA

You can use policies to configure your ESET product the same way you would from within the Advanced setup window of the product GUI. Unlike policies in Active Directory, ERA Policies cannot carry any script or series of commands.

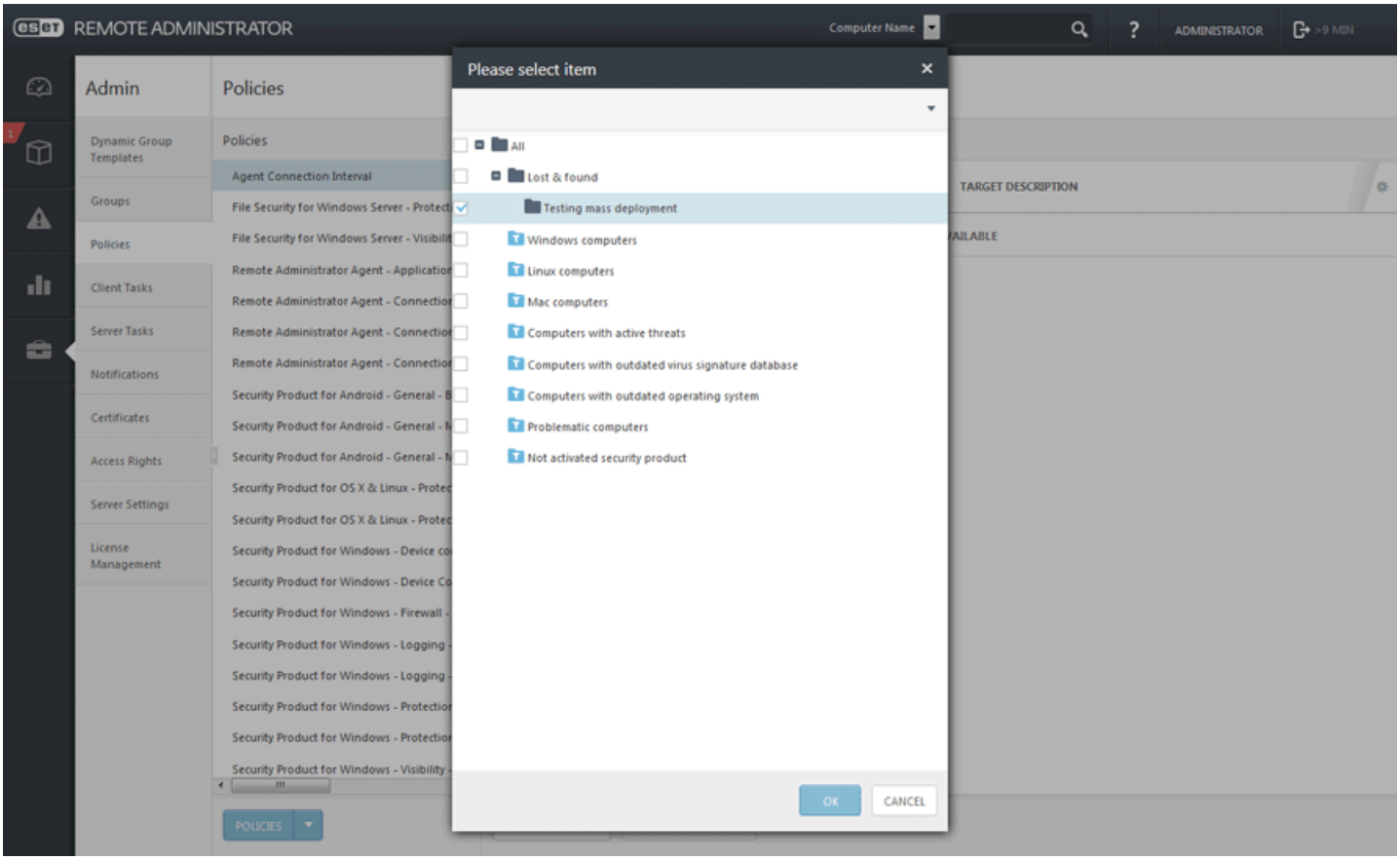
6.1.2.6 Assign Policy to Group

After a Policy is created, you can assign it to a **Static** or **Dynamic Group**. There are a two ways to assign a policy:

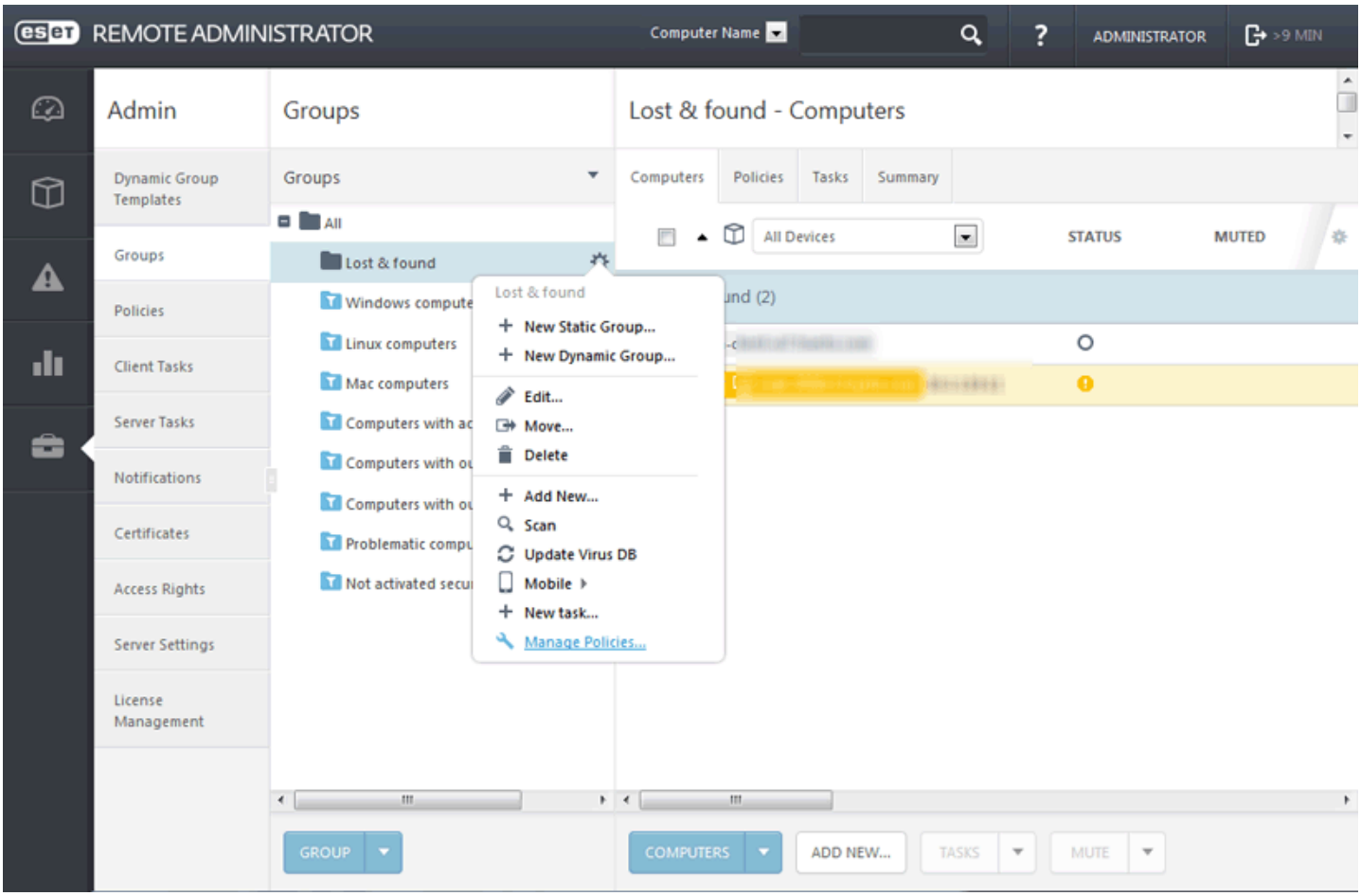
1. Under **Admin** > **Policies** > select a policy and click **Assign Group(s)**. Select a Static or Dynamic Group and click **OK**.



Select **Group** from the list.



2. Click **Admin** > **Groups** > **Group** or click the cogwheel icon next to the group name and select **Manage Policies**.

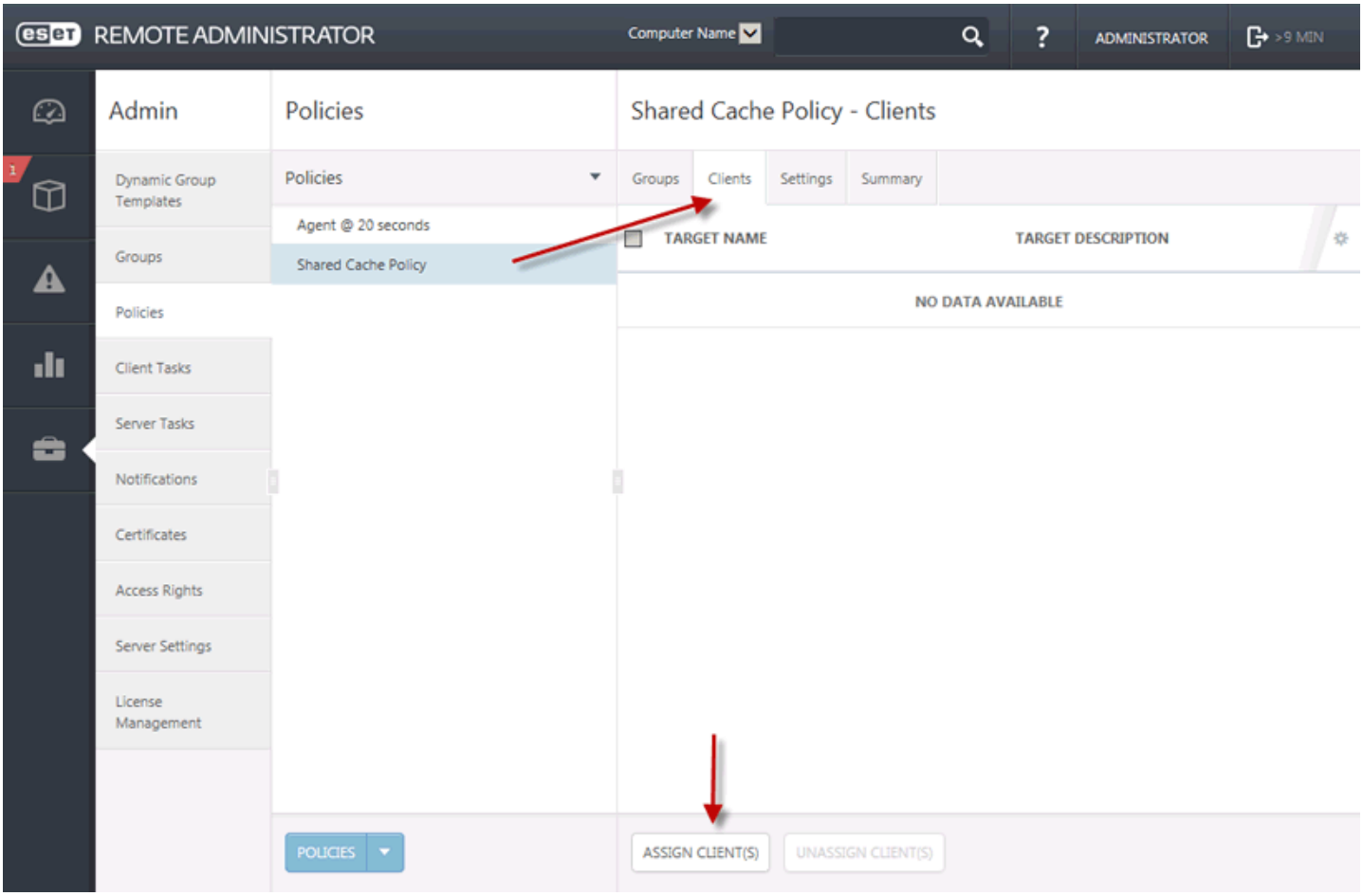


In the **Policy application order** window click **Add Policy**. Select the check box next to the policy that you want to assign to this group and click **OK**.
Click **Save**. To see what policies are assigned to a particular group, select that group and click the **Policies** tab to view a list of policies assigned to the group.

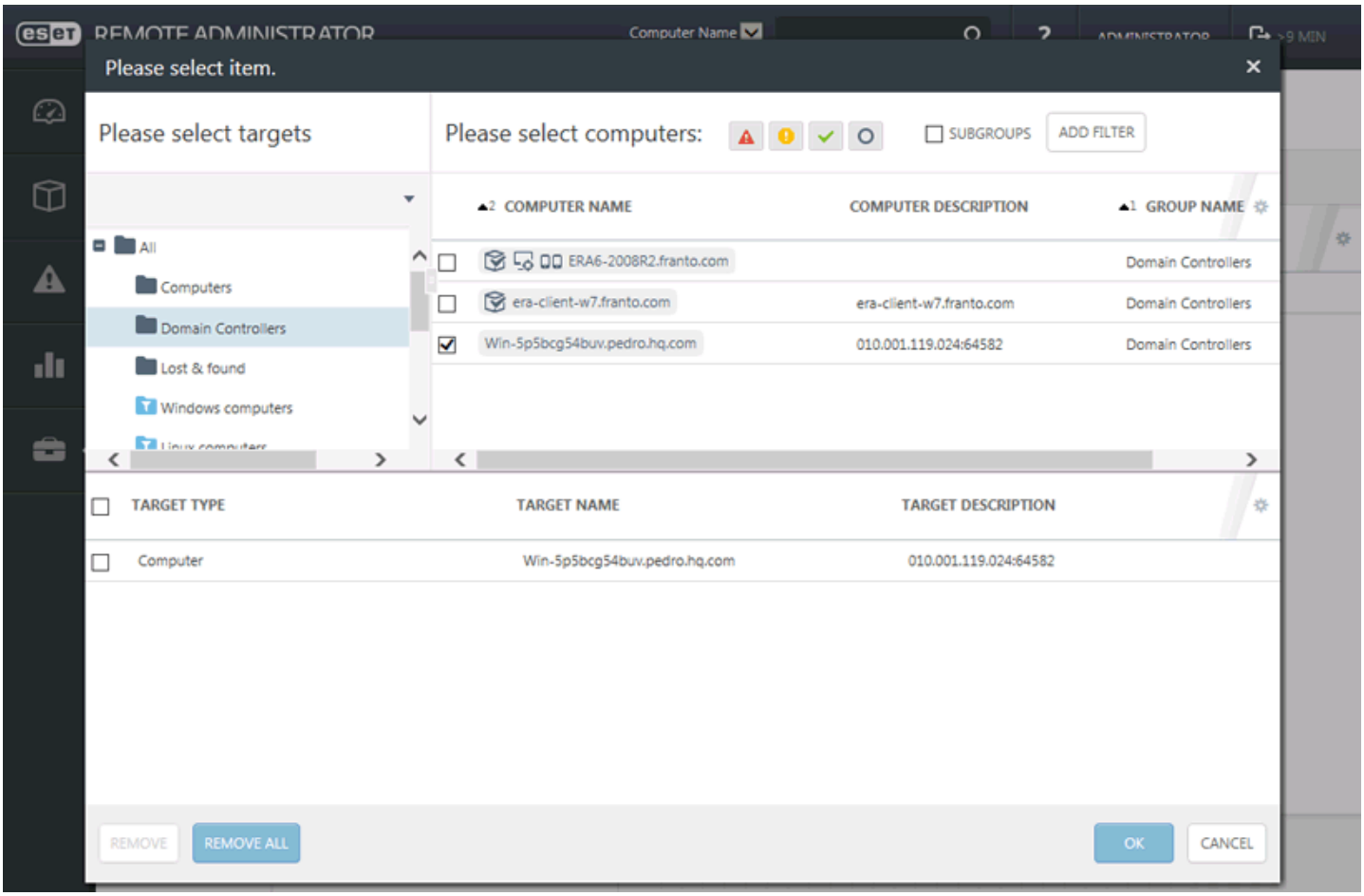
NOTE: For more information about policies, see the Policies chapter.

6.1.2.7 Assign a Policy to a Client

To assign a policy to a client workstation, click **Admin** > **Policies** select the **Clients** tab and click **Assign client(s)**.



Select your target client computer(s) and click **OK**. The policy will be assigned to all computers you have selected.



6.1.3 Client Tasks

To request an action from a client computer, you can use a **Client Task**. Client tasks can be assigned to groups or individual computers. Once created, the task is executed according to the scheduling plan. Since clients are not connected to the ERA Server all the time, it may take some time to propagate tasks to clients. For the same reason, it may also take some time for task execution results to get back to the ERA Server. The following pre-defined tasks are available for your convenience:

Each **Task Category** contains **Task Types:**

All Tasks

- **ESET Security Product**
  - Export Managed Products Configuration
  - On-Demand ScanProduct Activation
  - Quarantine Management
  - Run SysInspector Script
  - Software Install
  - SysInspector Log Request
  - Upload Quarantined File
  - Virus Signature Database Update
  - Virus Signature Database Update Rollback
- **ESET Remote Administrator**

Remote Administrator Components Upgrade

Reset Cloned Agent

Rogue Detection Sensor Database Reset

Stop Managing (Uninstall ERA Agent)

Operating System

Display Message

Operating System Update

Run Command

Software Install

Software Uninstall

Stop Managing (Uninstall ERA Agent)

Mobile

Anti-Theft Action

Device Enrollment

Display Message

Export Managed Products Configuration

On-Demand Scan

Product Activation

Software Install

Virus Signature Database Update

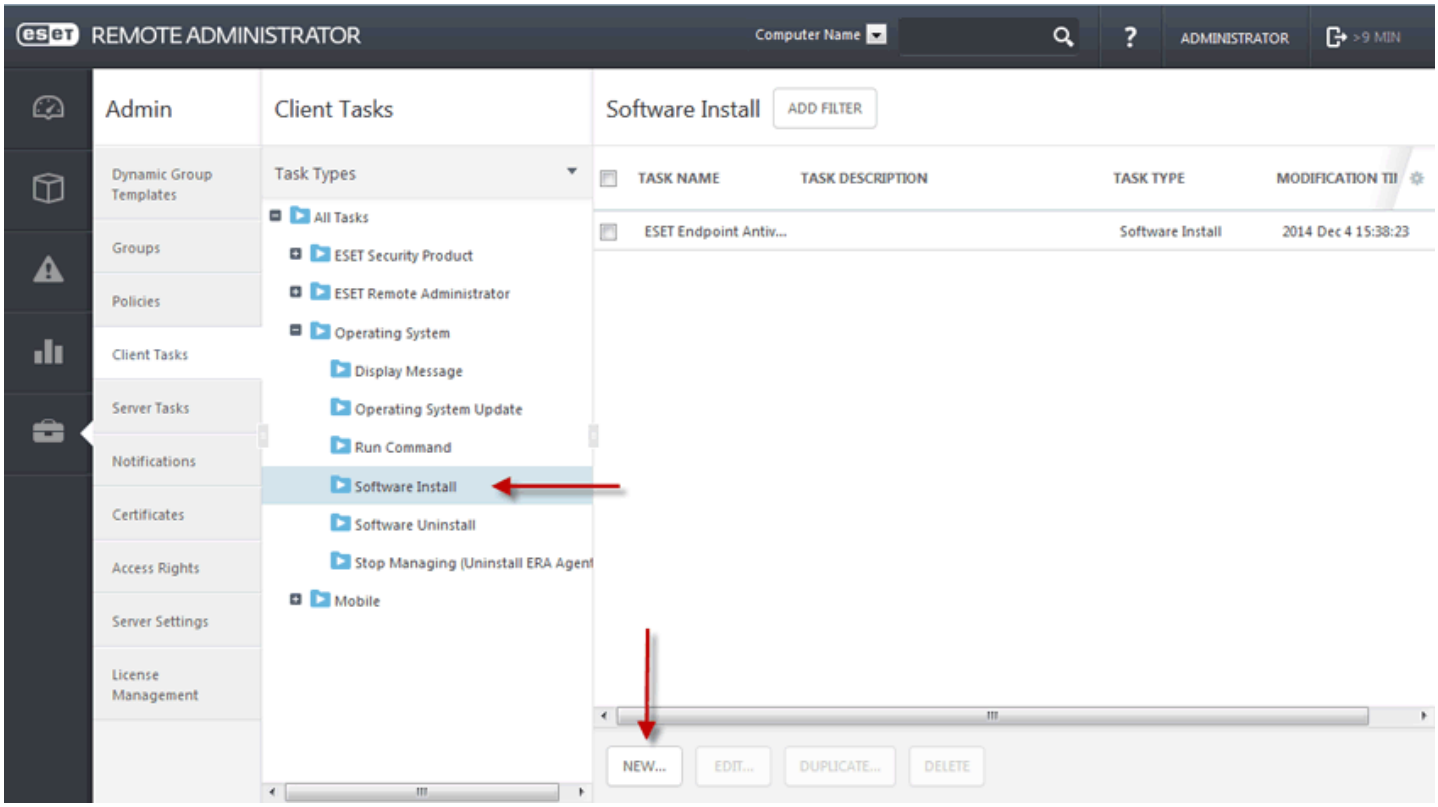
Stop Managing (Uninstall ERA Agent)

6.1.3.1 Client Task Wizard

Client tasks are created and managed from within the **Admin** tab. Click **Client tasks**, select a task from the **Task Types** list and then click **New.**

ESET security products can be installed remotely by clicking on the desired machine and selecting **New**, or by creating a new **Software Install** task under **Admin** > **Client Tasks** menu. Click **New...** to begin setting up your new task.

- Use following written instructions or watch Knowledgebase instructional video.

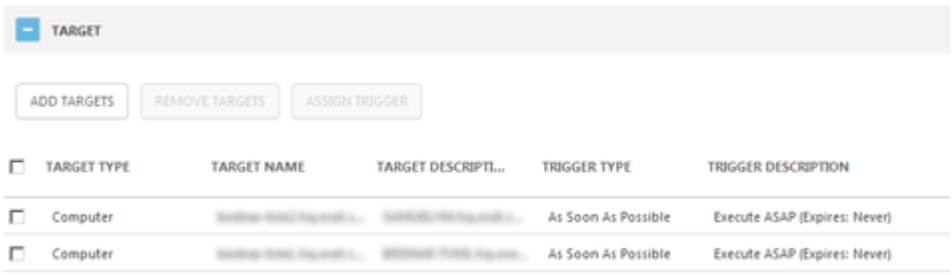


Basic

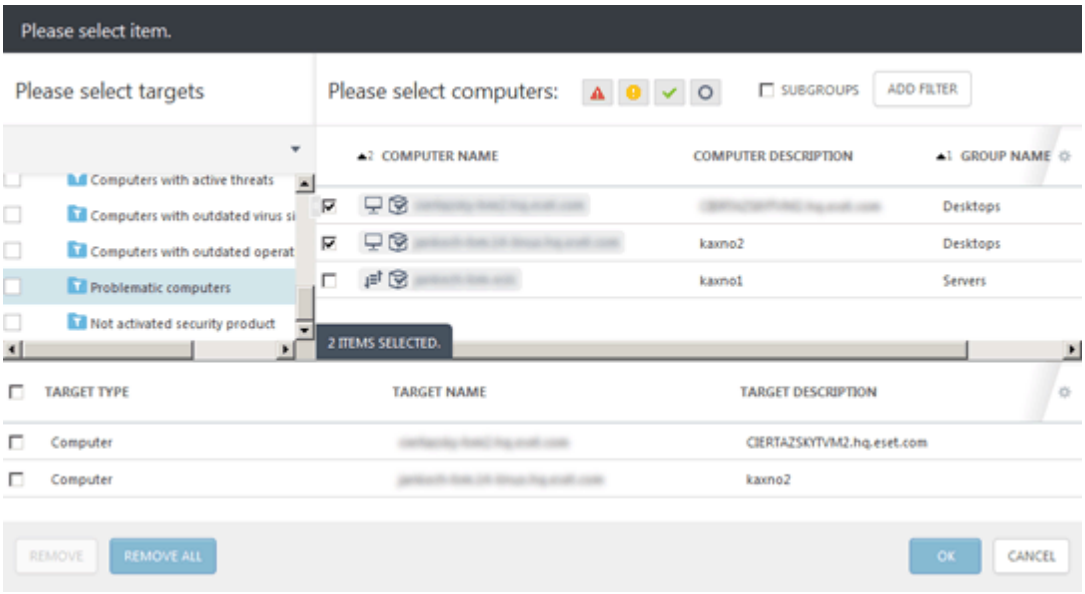
Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. Select the **Software Install** task and then click **Target**.

Target

Here you can specify the clients (individual computers or whole groups) that will receive this task.

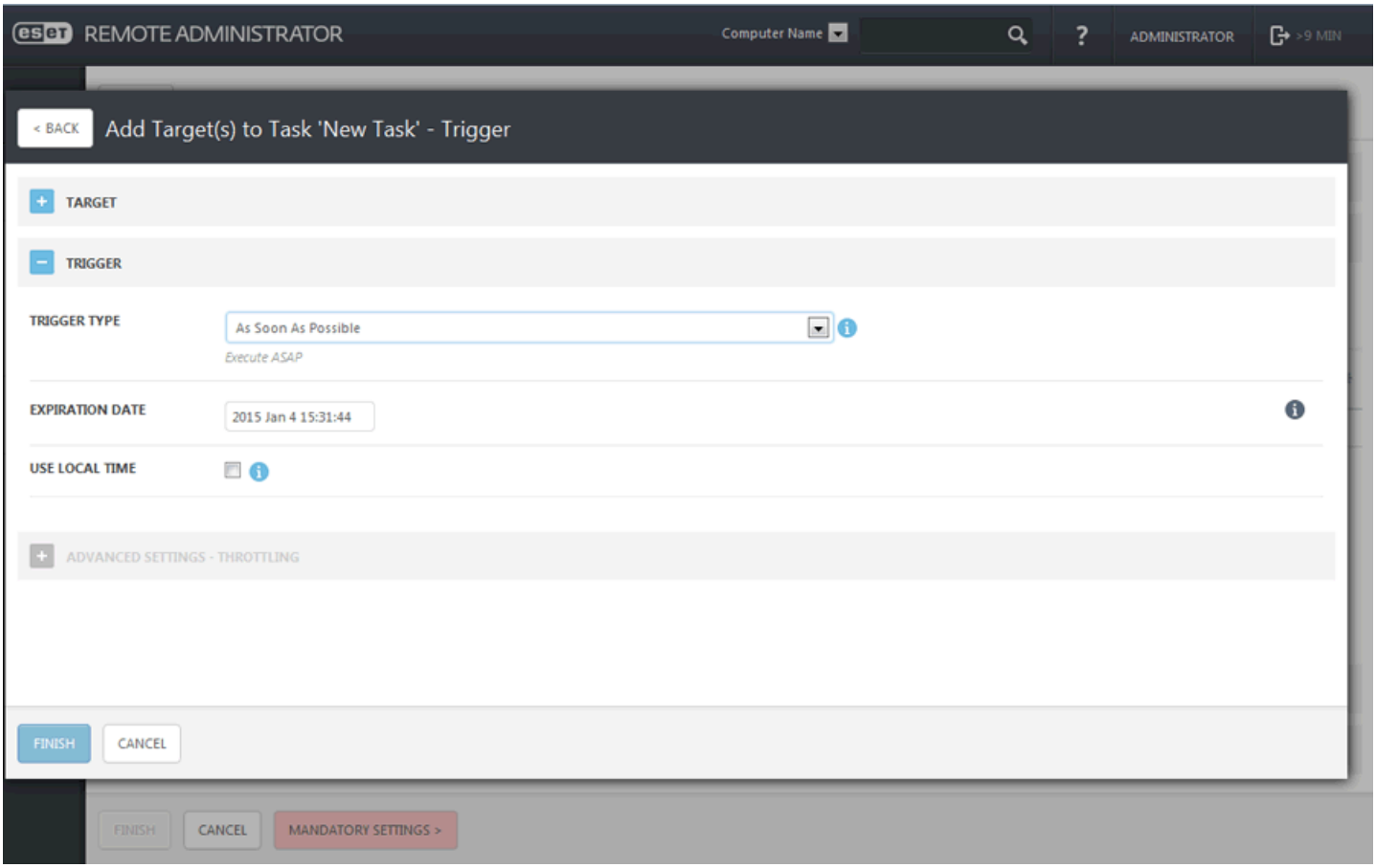


Click **Add targets** to display all Static and Dynamic Groups and their members.



Trigger

As a **Trigger** select **Execute ASAP**, this will send the task to clients immediately. The **Use Local Time** option refers to the local time of the client(s), not the server.



Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For now, we leave Throttling as it is and click **Finish** to create the new task.

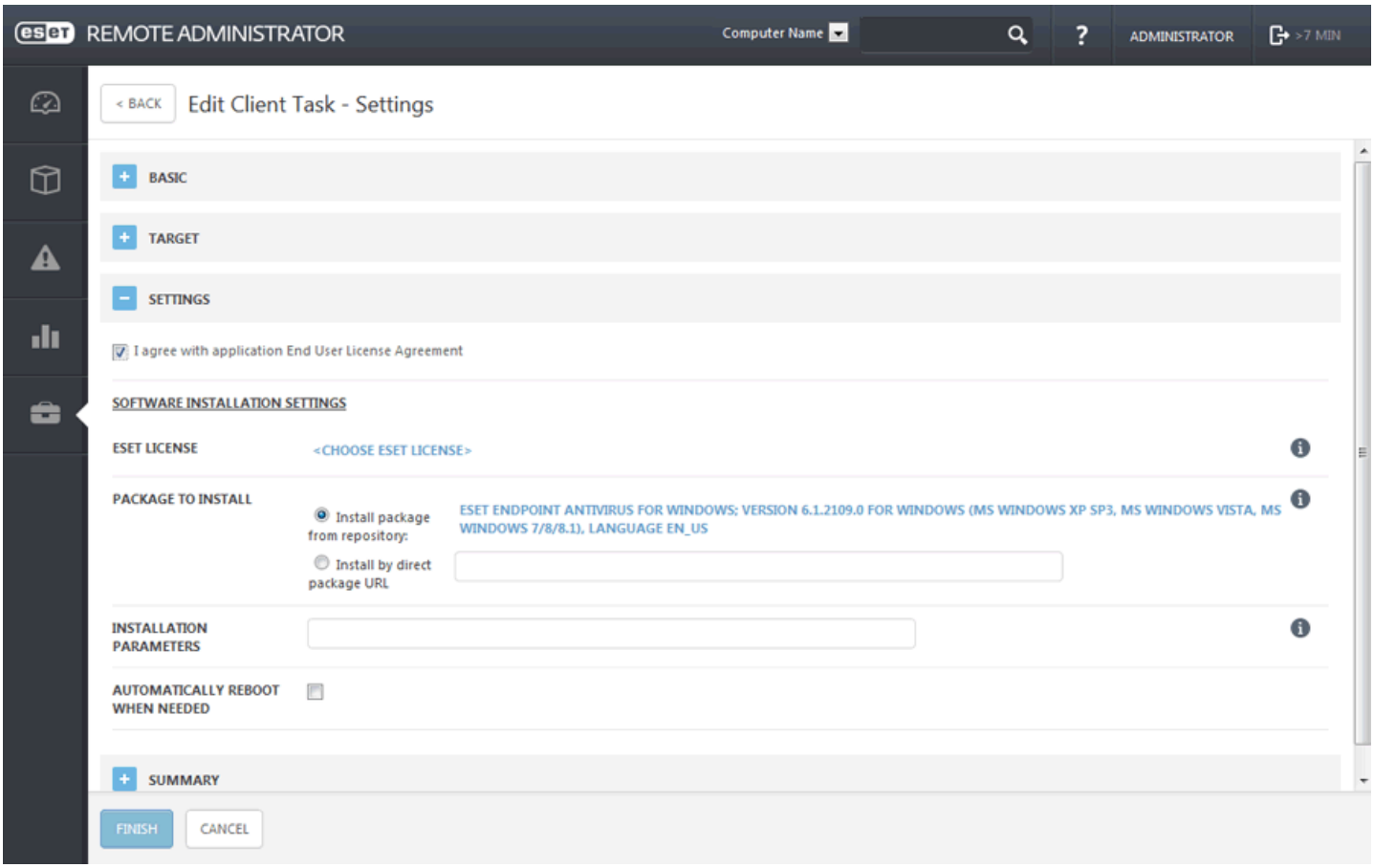
Settings

Click **<Choose ESET License>** and select the appropriate license for the installed product from the list of available licenses. Select the check box next to **I agree with application End User License Agreement** if you agree. See License Management or EULA for more information.

Click **<Choose package>** to select a installer package from the repository or specify a package URL. A list of available packages where you can select the ESET product you want to install (for example, ESET Endpoint Security) will be displayed. Select your desired installer package and click **OK**. If you want to specify installation package URL, type or copy and paste the URL into the text field (do not use URL that requires authentication).

NOTE: Please note, that both Server and Agent needs to have access to the internet, to be able to access the repository and perform the installation. If you do not have internet access, you can install the client software locally.

If you need to, you can specify Installation parameters, otherwise leave this field empty. Select the check box next to **Automatically reboot when needed** to force an automatic reboot of the client computer after installation. Alternatively, you can leave this option unchecked and the decision to restart can be made by someone using the client computer.



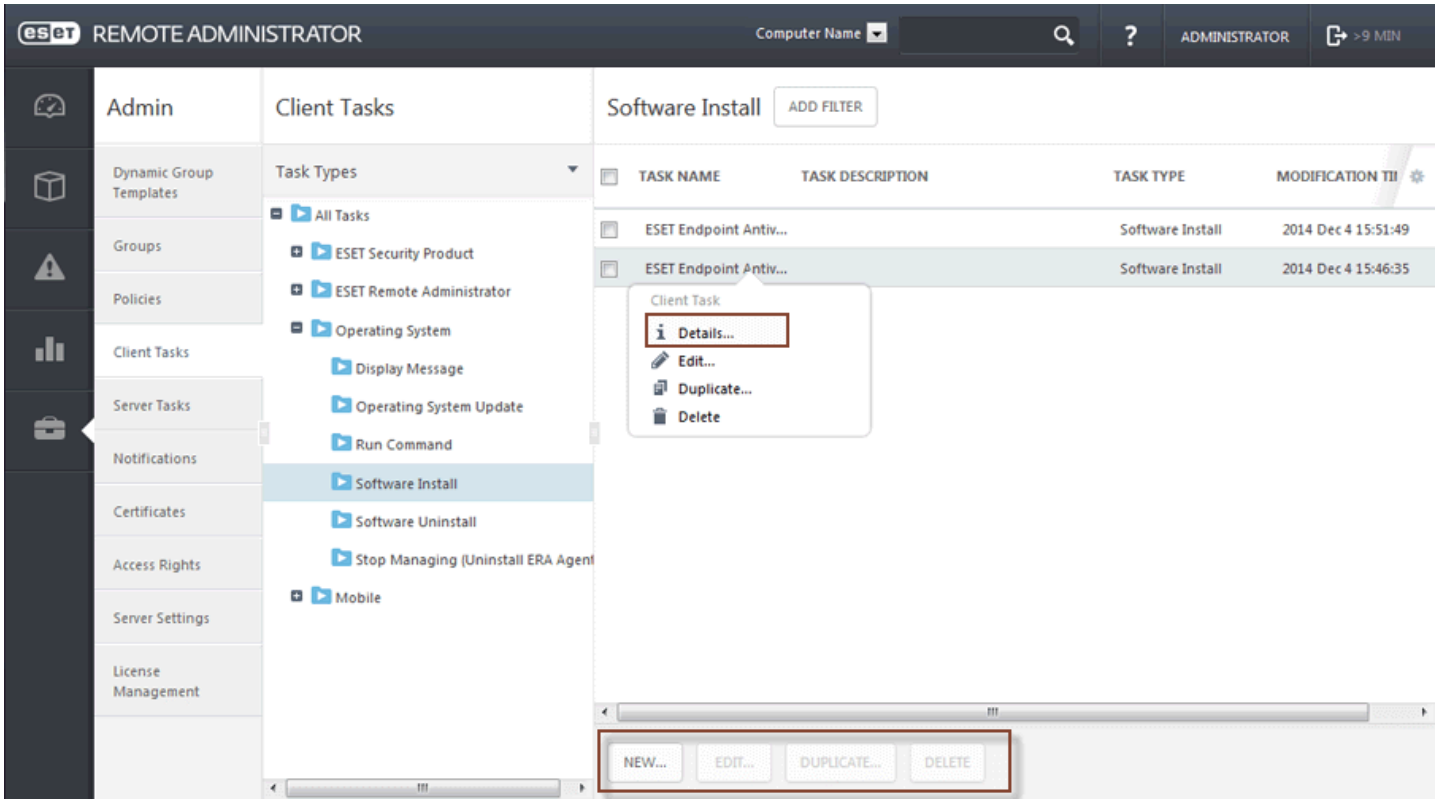
Summary

Review the summary of configured settings and click **Finish**. The task is now created and will be sent to the client(s).

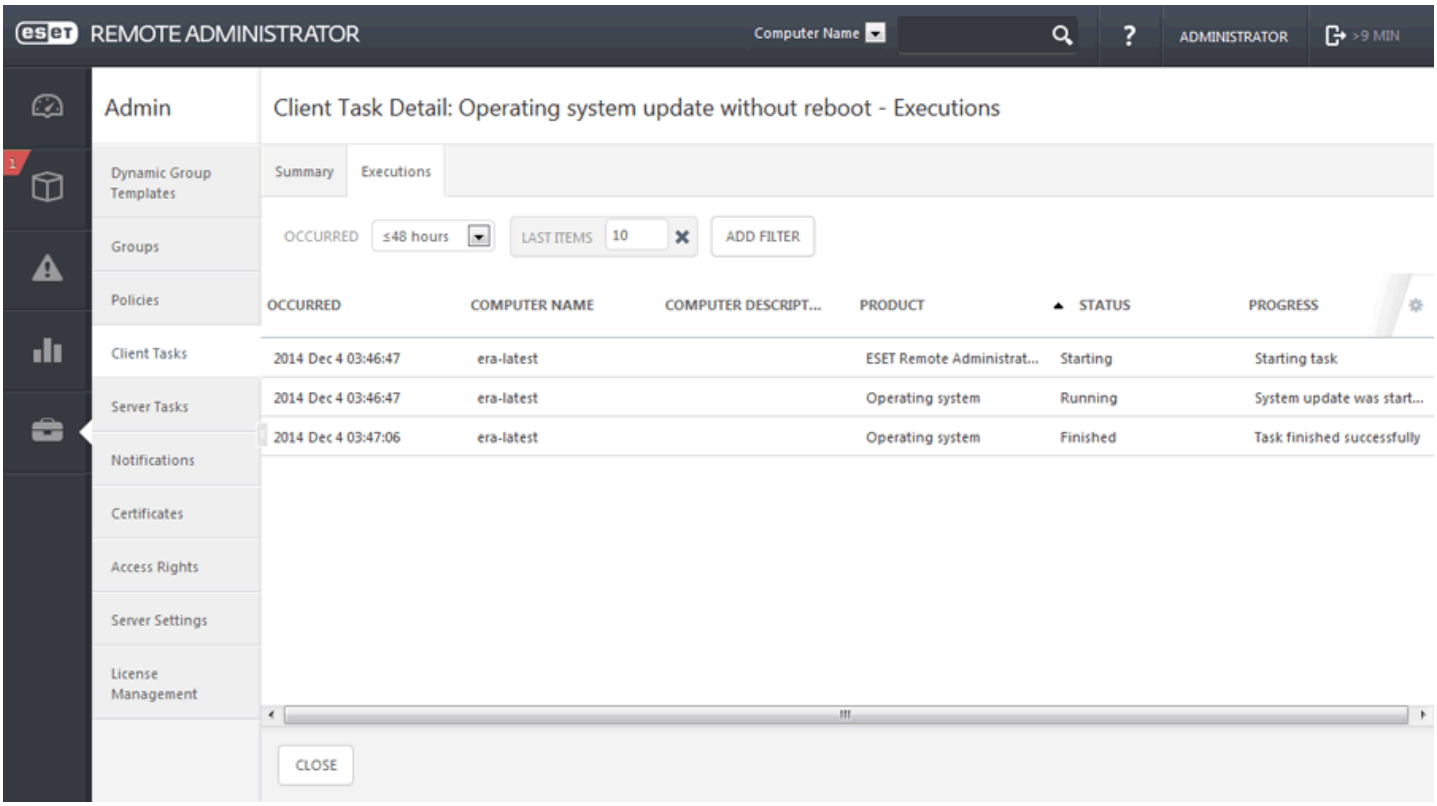
6.1.3.2 Manage Client Tasks

You can use Client Tasks to manage clients and their security products. There is a set of predefined tasks to cover the most common uses, or you can create custom tasks with specific settings.

- You can **Edit** existing tasks to make new ones. Editing existing tasks is useful when you only need to make small adjustments. For more unique tasks, it might be preferable to create a new task from scratch.
- **Duplicate -** A new client task will be added based on the selected task, a new name is required for the duplicate task.
- **Delete -** Removes the selected task(s) completely.



- **Details...** - will display the task configuration, **Summary**, and task **Executions.** (Occurred, Computer Name, Product, Status and Progress).



NOTE: When installing an older product, client task report displays information - Task delivered to the managed product.

6.1.3.2.1 On-Demand Scan

The **On-Demand Scan** task lets you manually run a scan on the client computer (separate from a regular scheduled scan).

Shutdown after scan - If you select this check box, the computer will shut down after scanning is finished.

Scan profile - You can select the profile you want from the drop-down menu:

- **In-depth Scan** - This is a pre-defined profile on the client, it is configured to be the most thorough scan profile and checks the whole system but also requires the most time and resources.
- **Smart scan -** Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Smart scan is it is easy to operate and does not require detailed scanning configuration. Smart scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value.
- **Scan From Context Menu** - Scans a client using a pre-defined scan profile, you can customize the scan targets.
- **Custom Profile** - Custom scan lets you specify scanning parameters such as scan targets and scanning methods. The advantage of a Custom scan is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which make it easy to repeat the scan using the same parameters. A profile must be created prior to running the task with the custom profile option. Once you select a custom profile from the drop-down menu, type the exact name of the profile into the **Custom profile** field.

Cleaning

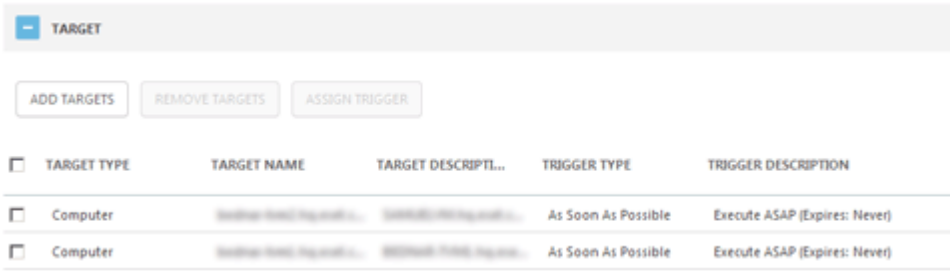
By default, **Scan with cleaning** is selected. This means that when infected objects are found, they are cleaned automatically. If this is not possible, they will be quarantined.

Scan Targets

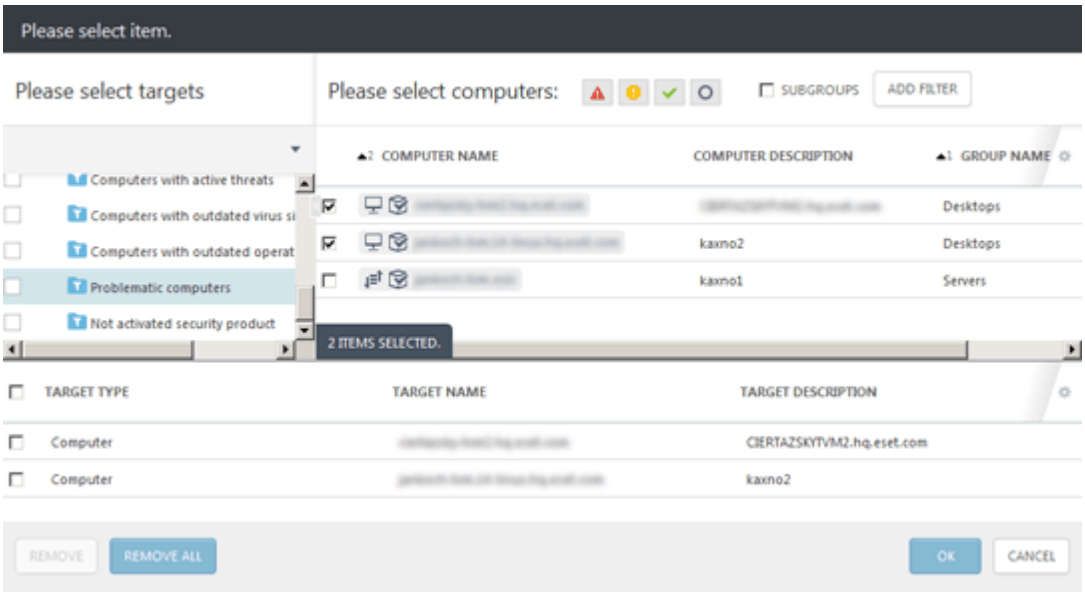
This option is also selected by default. Using this setting, all targets specified in the scan profile are scanned. If you deselect this option, you need to manually specify scan targets in the **Add Target** field. Type the scan target into the text field and click **Add**. The target will be displayed in the **Scan targets** field below.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Summary

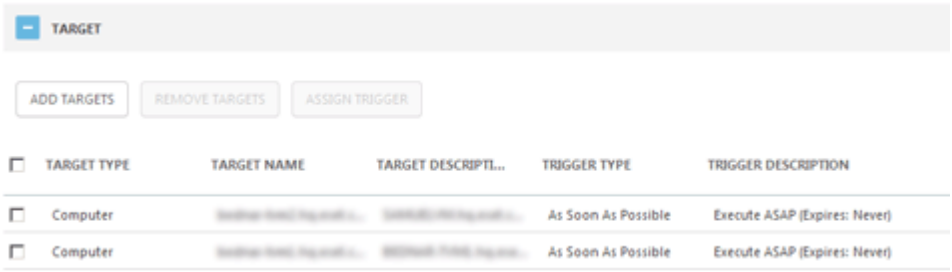
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.2 Operating System Update

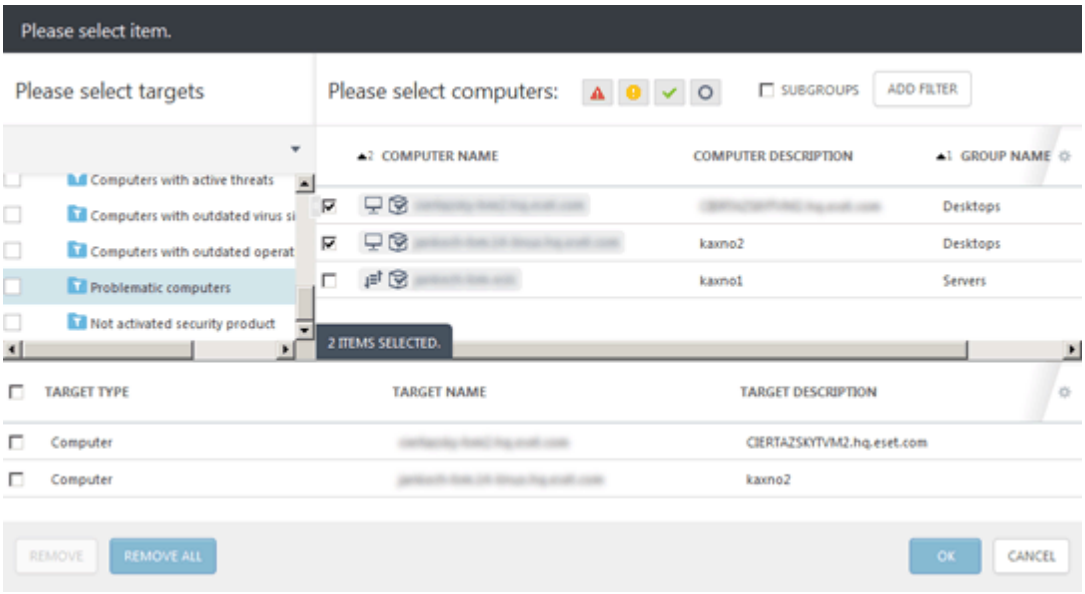
The **System Update** task is used to update the operating system of the client computer. This task can trigger the operating system update on Windows, Mac and Linux operating systems.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Allow Reboot** - This option applies only to windows operating systems, and causes the client computer to reboot once an update is installed.

Summary

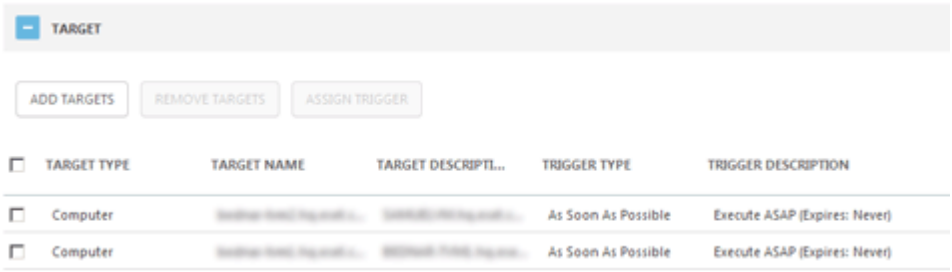
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.3 Quarantine Management

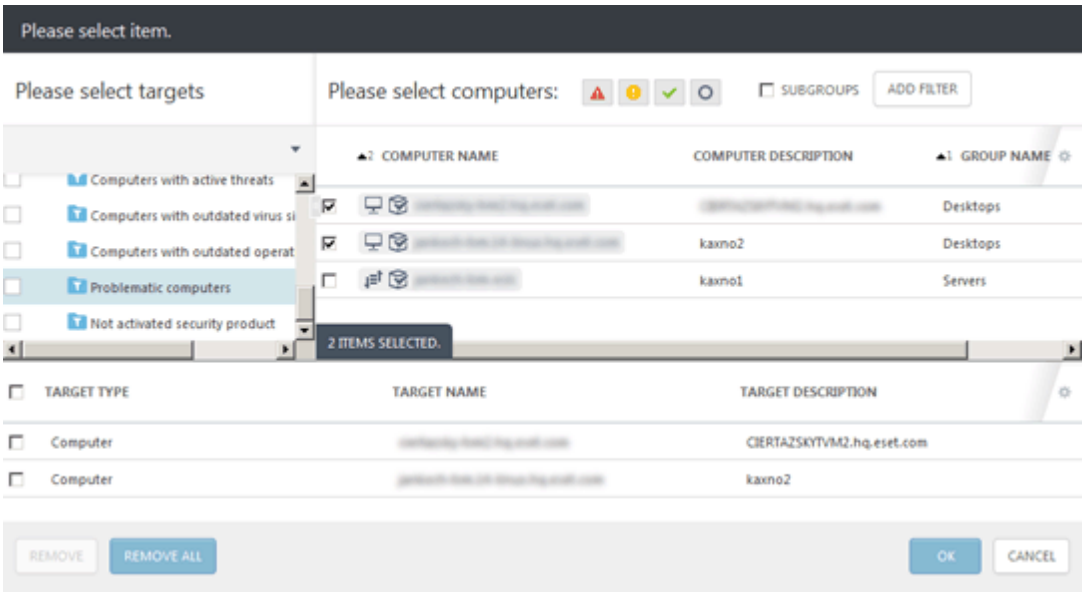
The **Quarantine management** task is used to manage objects in the ERA Server quarantine - infected or suspicious objects found during the scan.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

Quarantine management settings

- **Action** - Select the action to be taken with the object in Quarantine.

Restore object (restores the object to its original location, but it will be scanned and if the reasons for the Quarantine persist, the object will be quarantined again)
Restore object and exclude in future (restores the object to its original location and it will not be quarantined again).
Delete object (deletes the object completely).

- **Filter type** - Filter the objects in the Quarantine based on the criteria defined below. Either based on the Hash string of the object or Conditions.

Hash filter settings

Add hash items into the field. Only known objects can be entered, for example, an object that has already been quarantined.

Conditional filter settings

- **Occurred from/to** - Define the time range, when the object has been quarantined.
- **Minimal/maximal size (bytes)** - Define the size range of the quarantined object (in bytes).
- **Threat name** - Select a threat from the quarantined items list.
- **Object name** - Select an object from the quarantined items list.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

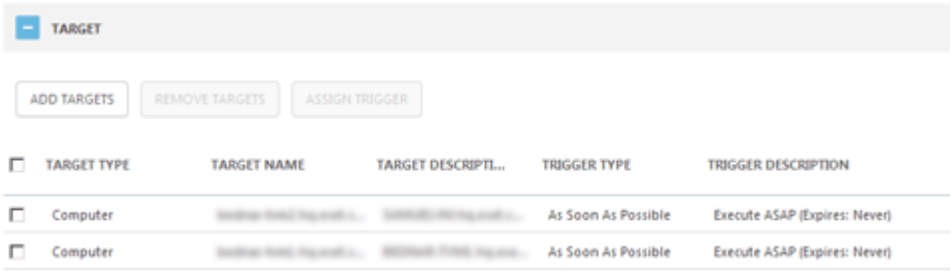
6.1.3.2.4 Rogue Detection Sensor Database Reset

The **Rogue Detection Sensor Database Reset** task is used to reset the RD Sensor search cache. The task deletes the cache and the search results will be stored again. This task does not remove detected computers. This task is useful when detected computers are still in the cache and are not reported to the server.

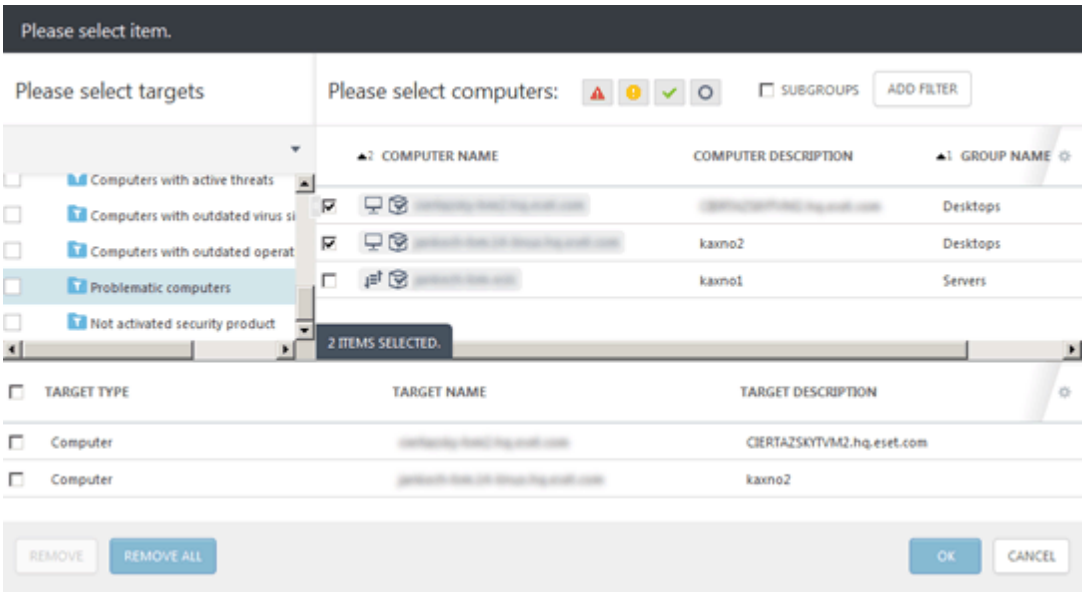
NOTE: Settings are not available for this task.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Summary

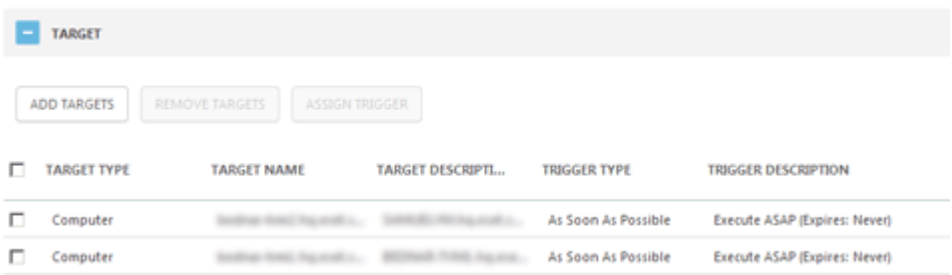
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.5 Remote Administrator Components Upgrade

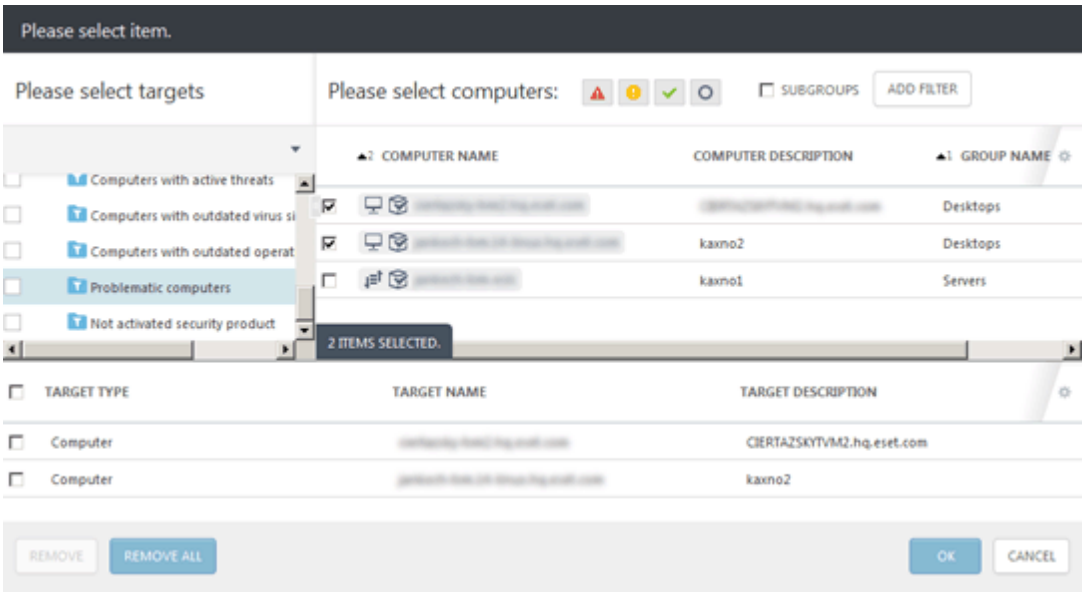
The **Remote Administrator Components Upgrade** task is used to upgrade ERA core components (Agent, Proxy, Server and MDM) installed on a client to the version compatible with a specific ERA Server (reference server).

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Reference Remote Administrator Server** - Select ERA Server version from the list. All ERA components will be upgraded to versions compatible with the selected server.
- **Automatically reboot when needed** - You can force a reboot of the client operating system, if the installation requires so.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

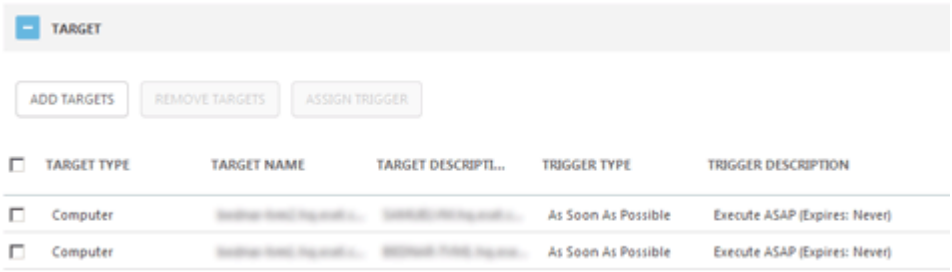
6.1.3.2.6 Reset Cloned Agent

The **Reset Cloned Agent** task can be used to distribute the ESET Agent in your network via a pre-defined image. Cloned Agents have the same SID, which can cause problems (multiple Agents with the same SID), to resolve this, use the **Reset Cloned Agent** task to reset the SID and assigns Agents a unique identity.

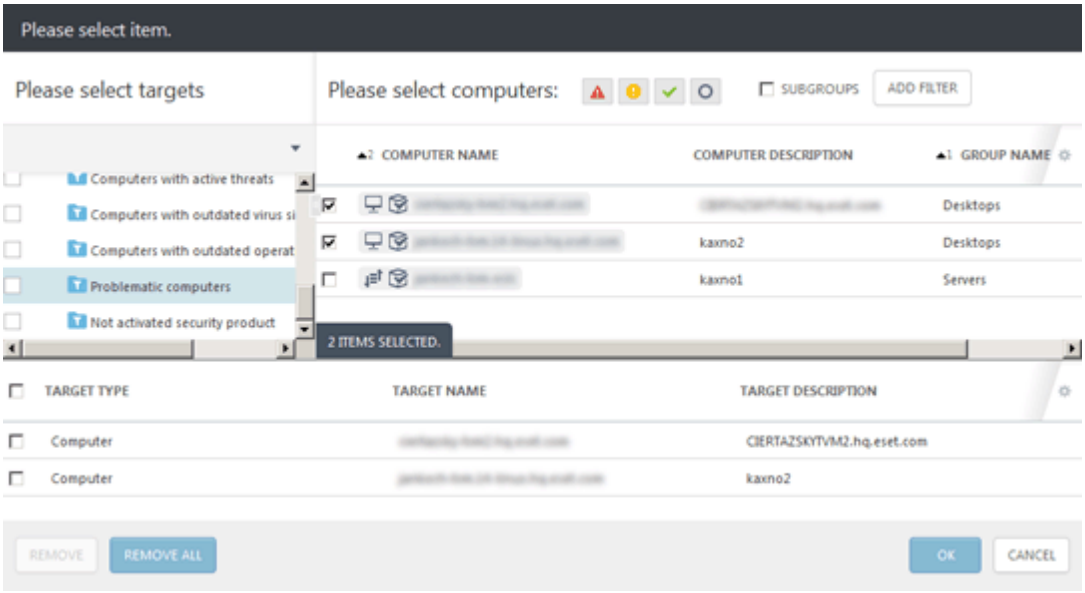
NOTE: Settings are not available for this task.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Summary

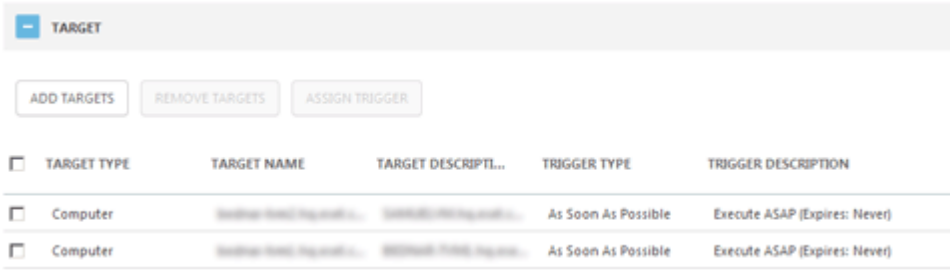
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.7 Run Command

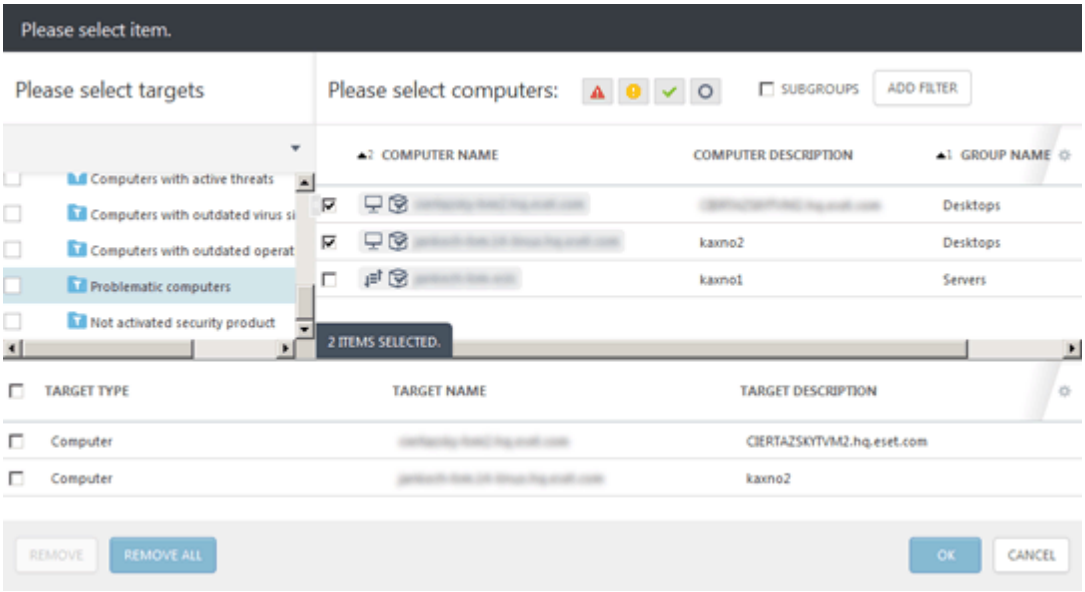
The **Run command** task can be used to execute specific command line instructions on the client. The administrator can specify the command line input to run.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Command line to run** - Enter a command line you want to run on the client(s).
- **Working directory** - Enter a directory where the command line above will be executed.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

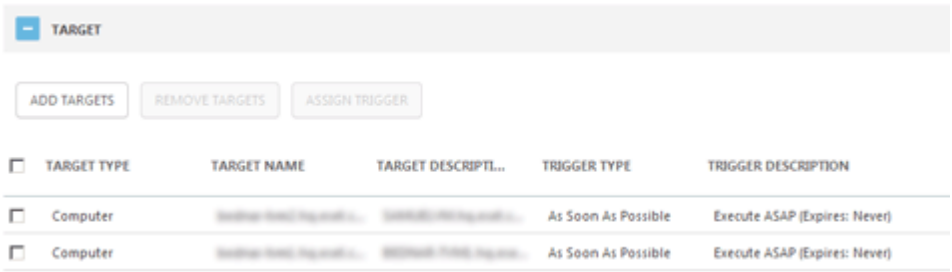
6.1.3.2.8 Run SysInspector Script

The **Run SysInspector Script** task is used to remove unwanted objects from the system. A **SysInspector Script** needs to be exported from ESET SysInspector prior to using this task. After you export the script, you can mark objects you want to remove and run the script with the modified data - the marked objects will be deleted.

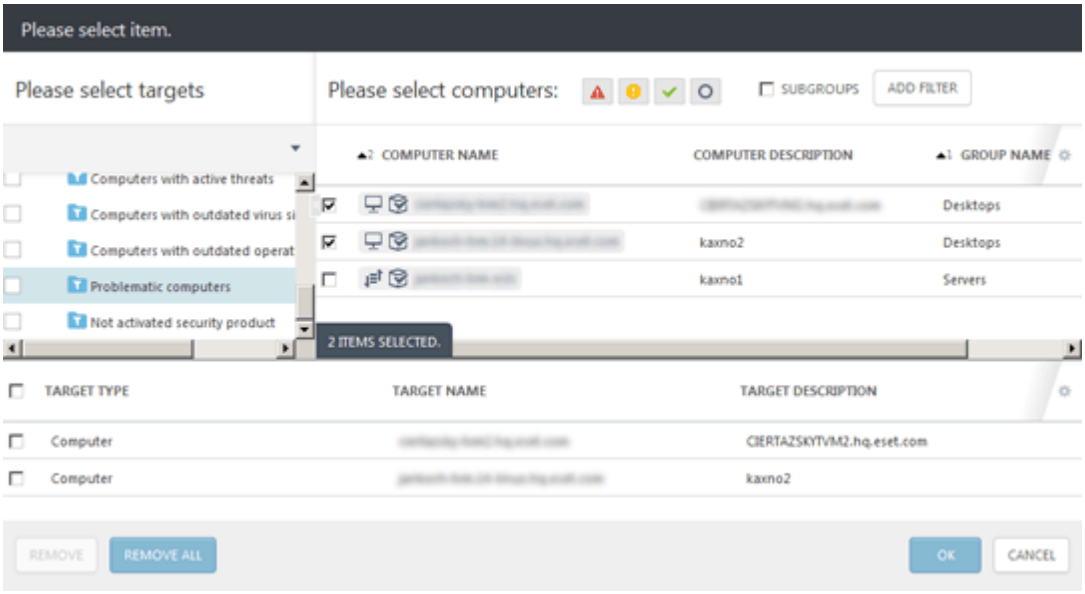
NOTE: Once the task is finished, you can review the results in a report.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **SysInspector Script** - Click **Browse** to navigate to the service script. The service script needs to be created prior to running this task.
- **Action** - You can either **Upload** to, or **Download** a script from the ERA Console.

Summary

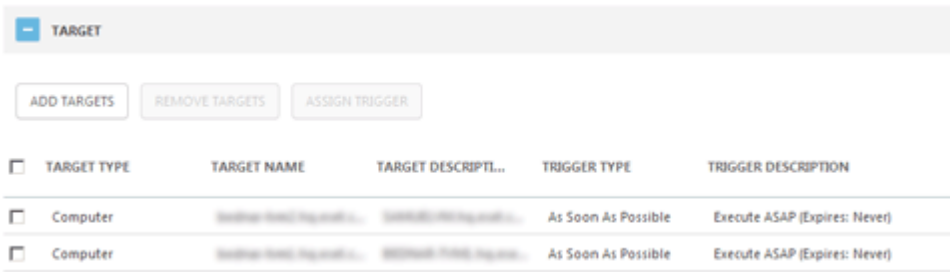
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.9 Software Install

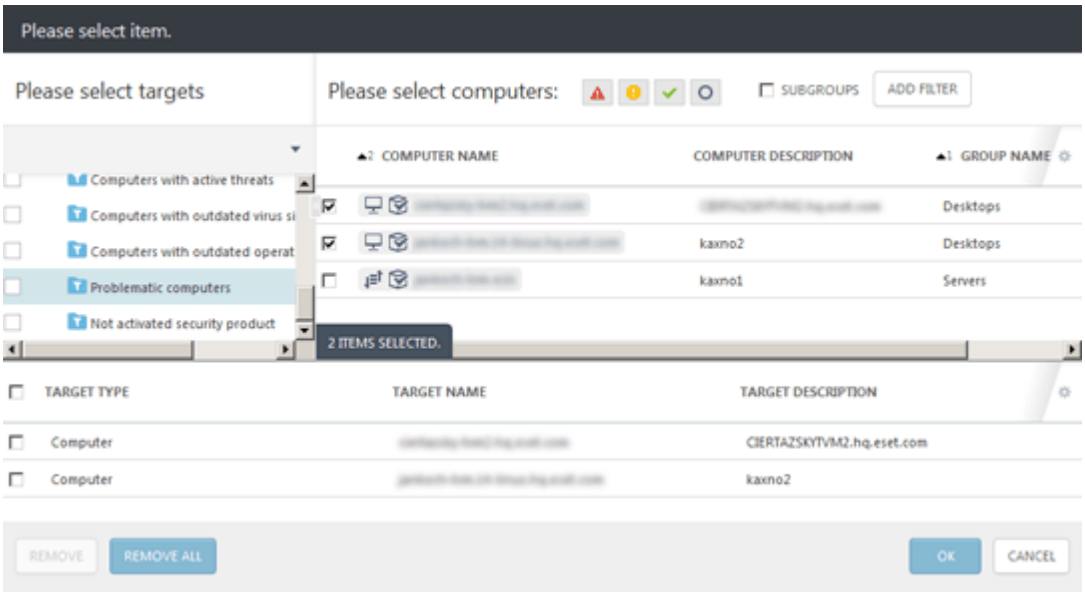
The **Software Install** task is used to install software on your client computers. It is primarily intended to install ESET products, but you can use it to install any software you like. Use following written instructions or watch Knowledgebase instructional video.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

Click **<Choose ESET License>** and select the appropriate license for the installed product from the list of available licenses. Select the check box next to **I agree with application End User License Agreement** if you agree. See License Management or EULA for more information.

Click **<Choose package>** to select a installer package from the repository or specify a package URL. A list of available packages where you can select the ESET product you want to install (for example, ESET Endpoint Security) will be displayed. Select your desired installer package and click **OK**. If you want to specify installation package URL, type or copy and paste the URL into the text field (do not use URL that requires authentication).

NOTE: Please note, that both Server and Agent needs to have access to the internet, to be able to access the repository and perform the installation. If you do not have internet access, you can install the client software locally.

If you need to, you can specify Installation parameters, otherwise leave this field empty. Select the check box next to **Automatically reboot when needed** to force an automatic reboot of the client computer after installation. Alternatively, you can leave this option unchecked and the decision to restart can be made by someone using the client computer.

Summary

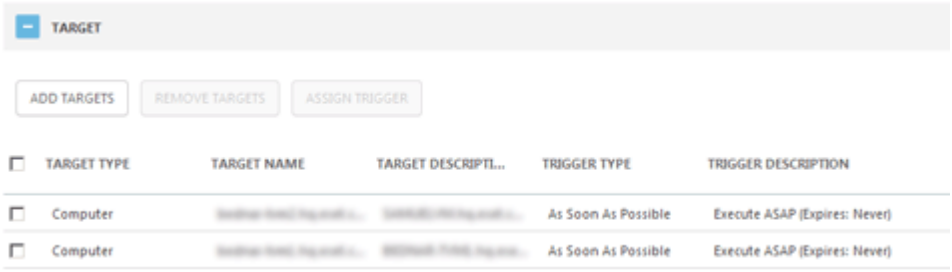
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.10 Software Uninstall

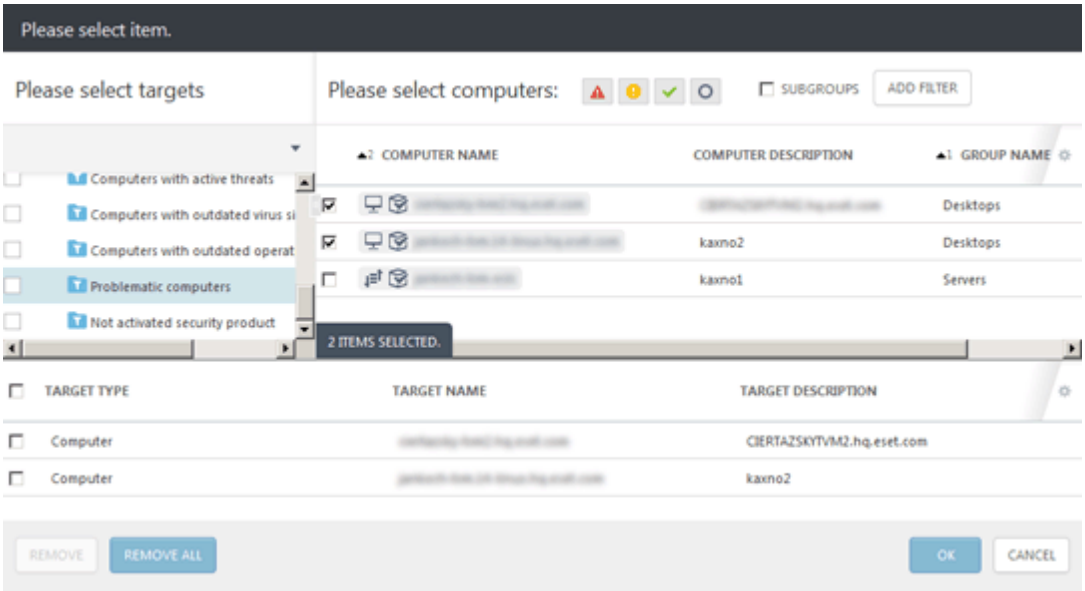
The **Software Uninstall** task is used to uninstall ESET products from clients when they are no longer wanted/needed. If you are uninstalling the ERA Agent, ESET products managed by that Agent may retain some settings after the Agent is uninstalled.
We recommend that you reset some settings (for example, password protection) to default settings using a policy before the device is removed from management. Also, all tasks running on the Agent will be abandoned. The **Running**, **Finished** or **Failed** execution status of this task may not be displayed accurately in ERA Web Console depending on replication.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

Software Uninstallation Settings

- **Uninstall** - **Application from list:**

Package name - Select an ERA component or a client security product. All packages installed on the selected client(s) are displayed in this list.
Package version - You can either remove a specific version (sometimes, a specific version can cause problems) of the package, or uninstall all versions of a package.
Automatically reboot when needed - You can force a reboot of the client operating system if it is required for uninstallation.

- **Uninstall** - **Third party antivirus software (Built with OPSWAT) -** For a list of compatible AV Software, see our Knowledgebase article. This removal is different from the **Add or Remove Programs** uninstallation. It uses alternative methods to remove third party antivirus software thoroughly including any residual registry entries or other traces.

Follow the step-by-step instructions in this article How do I remove third-party antivirus software from client computers using ESET Remote Administrator? (6.x) to send a task to remove third-party antivirus software from client computers.

Summary

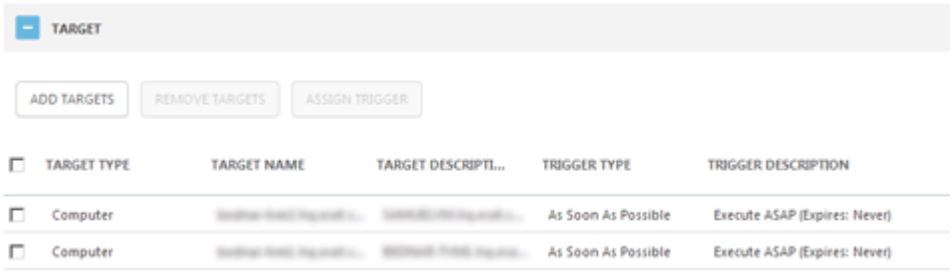
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.11 Product Activation

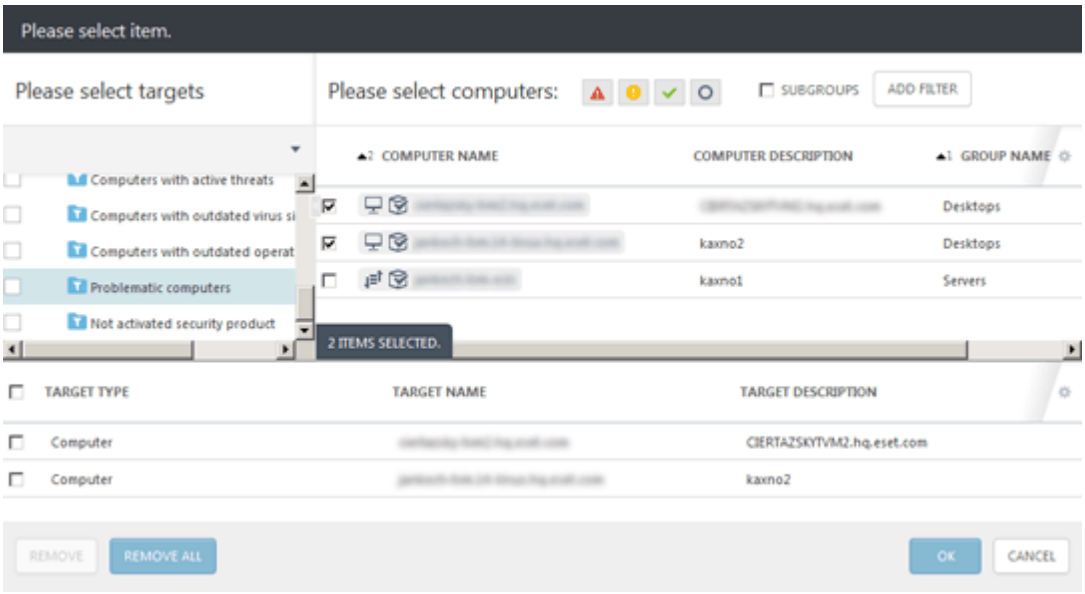
To activate an ESET product on a client computer, follow the steps below:

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

Product activation settings - Select a license for the client from the list. This license will be applied to products already installed on the client.

Summary

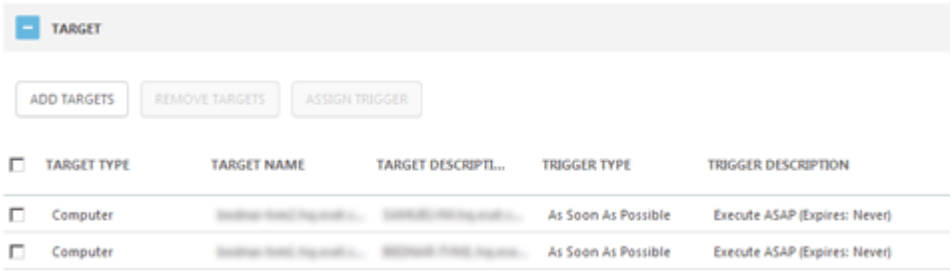
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.12 SysInspector Log Request

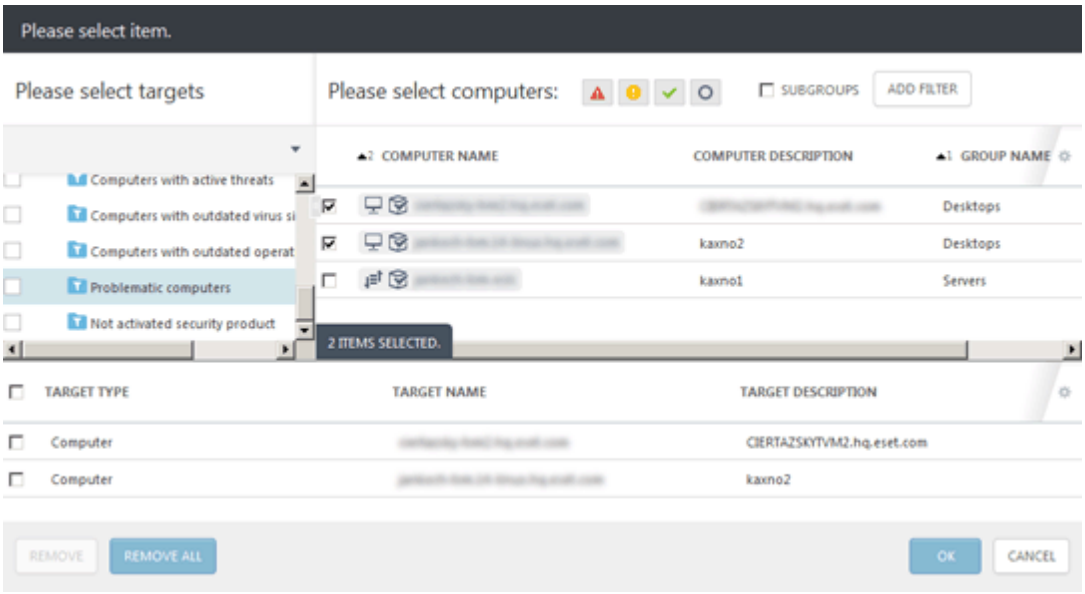
The **SysInspector Log Request** task is used to request the SysInspector log from a client security product, that has this function.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Store log on client** - Select this if you want to store the SysInspector log on the client as well as on the ERA Server. For example, when a client has ESET Endpoint Security installed, the log is usually stored under *C:\Program Data\ESET\ESET Endpoint Antivirus\SysInspector*.
- **Include comparison to the last snapshot prior to a specified time** - Allows you to compare the log being generated to logs from a specific period of time prior to this record. You can use the comparison information to identify differences and changes on the client.

Summary

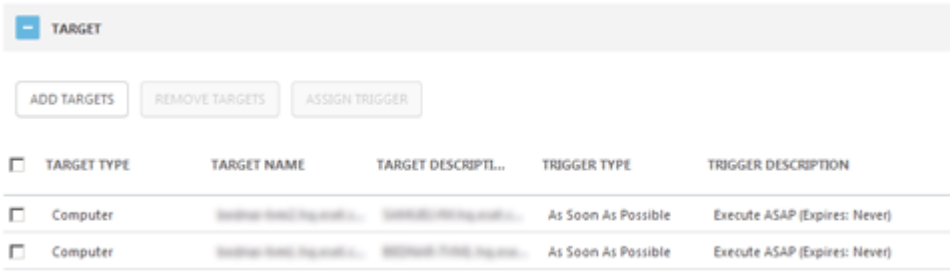
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.13 Upload Quarantined File

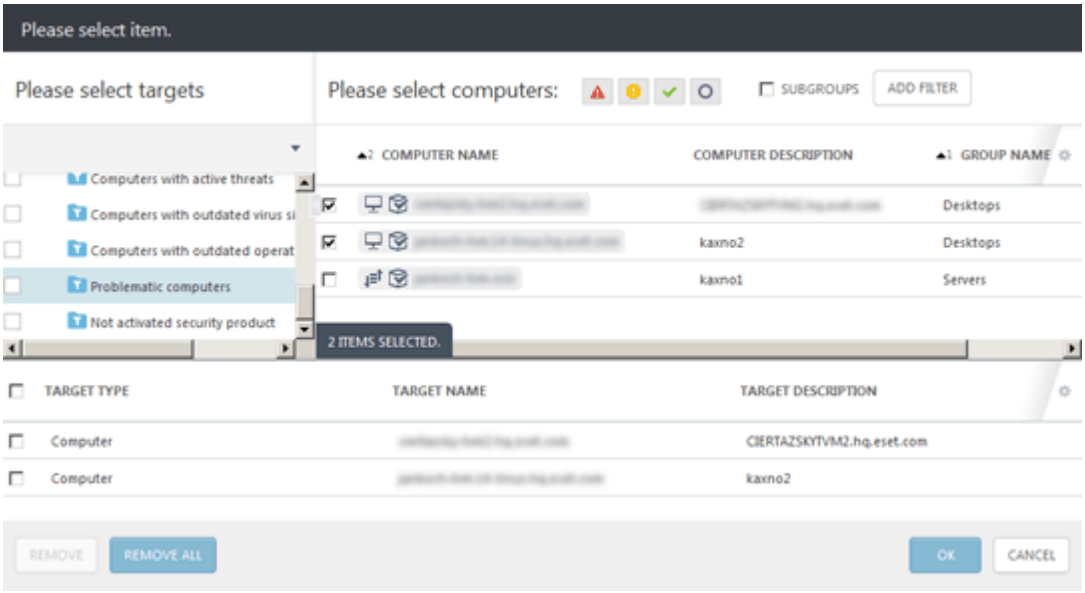
The **Upload Quarantined File** task is used to manage files quarantined on clients.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Quarantined object** - Select a specific object from the quarantine.
- **Object password** - Enter a password to encrypt the object for security reasons. Please note that password will be displayed in the corresponding report.
- **Upload path** - Enter a path to a location where you want to upload the object.
- **Upload username/password** - In case the location requires authentication (network share,etc.), enter the credentials to access this path.

Summary

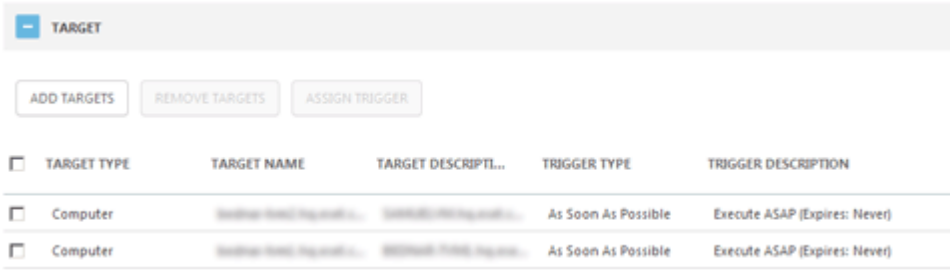
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.14 Virus Signature Database Update

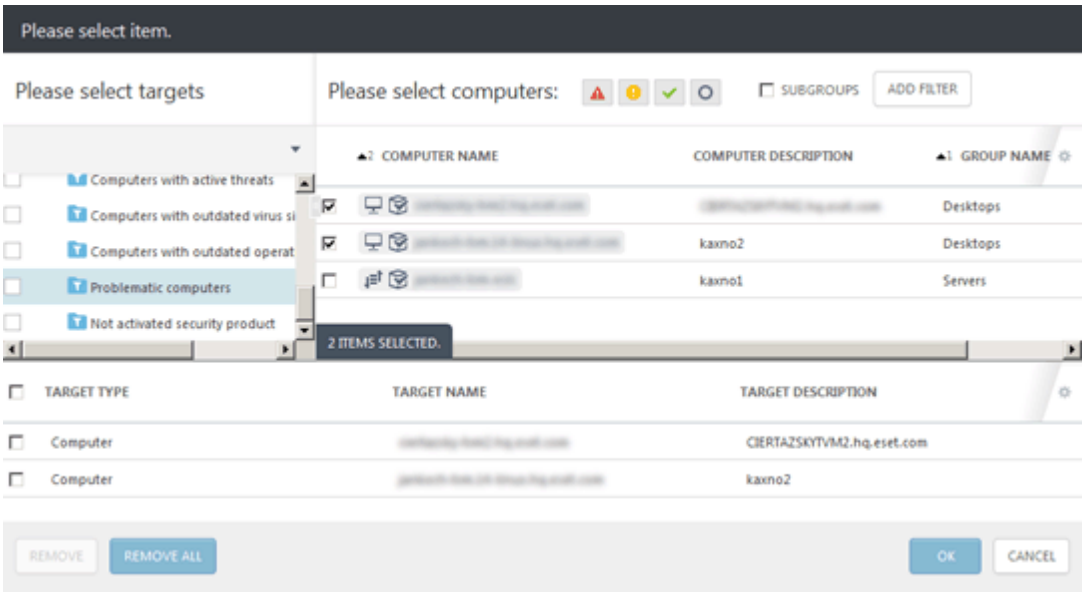
The **Product Update** task forces to update the virus signature database of the security product installed on the clients. This is a general task for all products on all systems.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Clear Update Cache** - This option deletes the temporary update files in the cache on the client, and can often be used to repair failed virus signature database update errors.

Summary

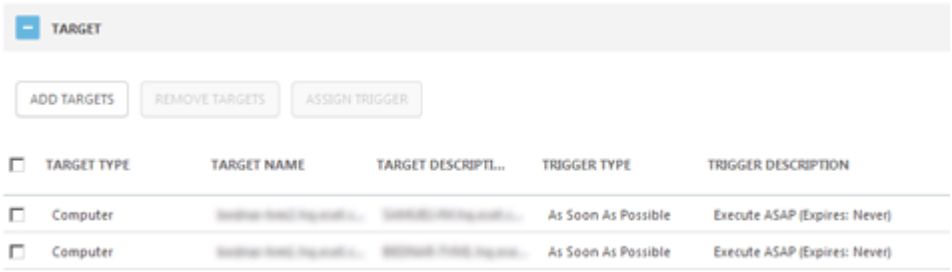
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.15 Virus Signature Database Update Rollback

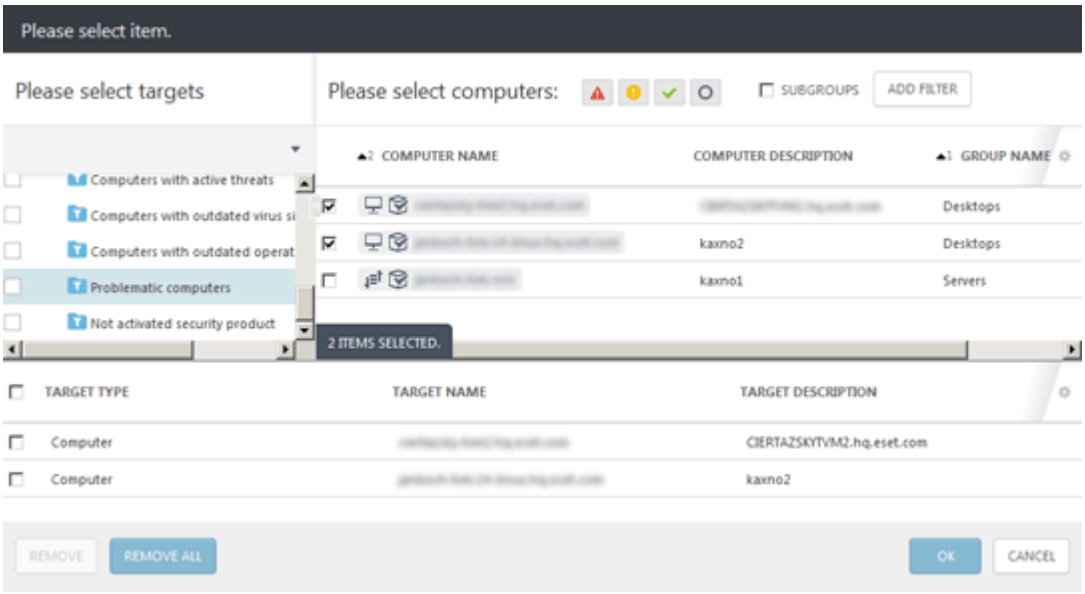
Sometimes a virus signature database update can cause issues, or you don't want to apply the update for all clients (for example, for testing or when using pre-release updates). In this case, you can use the **Virus Signature Database Update Rollback** task. When you apply this task, the virus signature database will be reset to the previous version.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

Here you can customize virus signature database update rollback settings.

Action

- **Enabled Updates** - Updates are enabled and the client will receive the next virus signature database update.
- **Rollback and Disable Updates for Next** - Updates are disabled for the specific time period in the **Disable interval** drop-down menu - 24/36/48 hours or until revoked. Be careful when using the **Until revoked** option, as this presents a security risk.

Summary

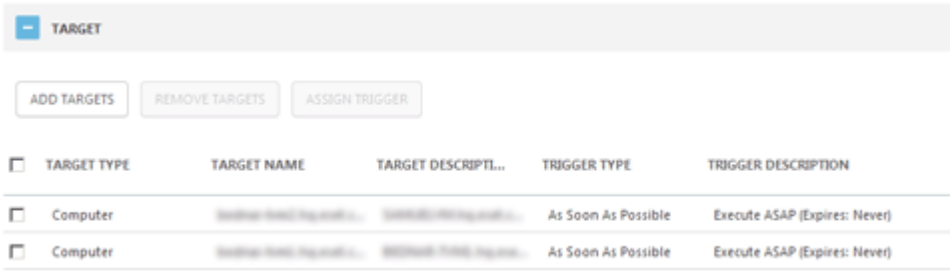
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.16 Display Message

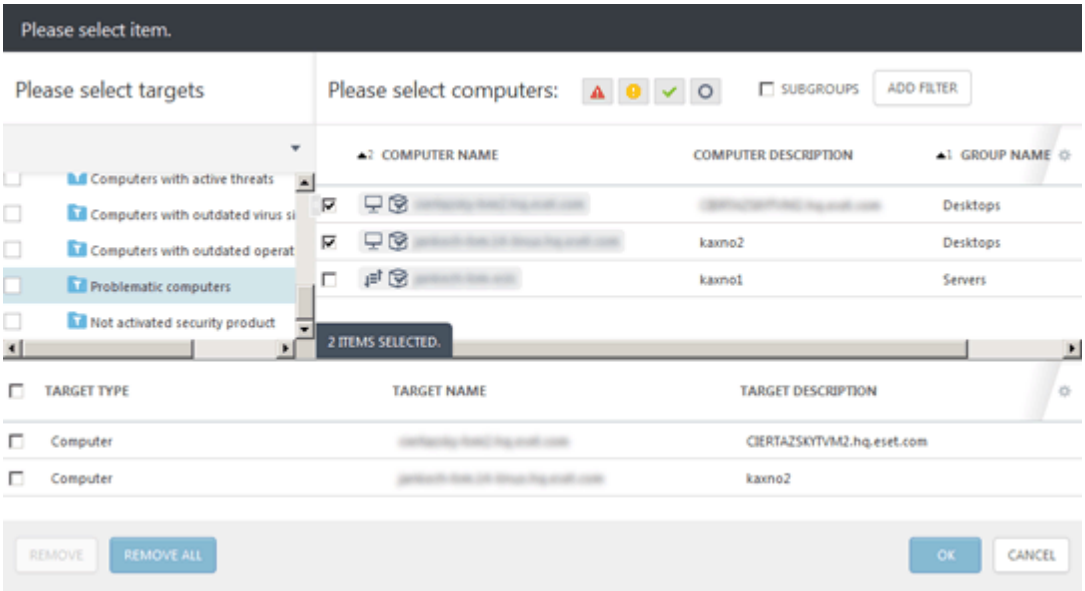
This functionality lets you send a message to any device (client computer, tablet, mobile, etc.). The message will be displayed on-screen to inform the user.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

You can enter a **Title** and type in your **Message**.

Summary

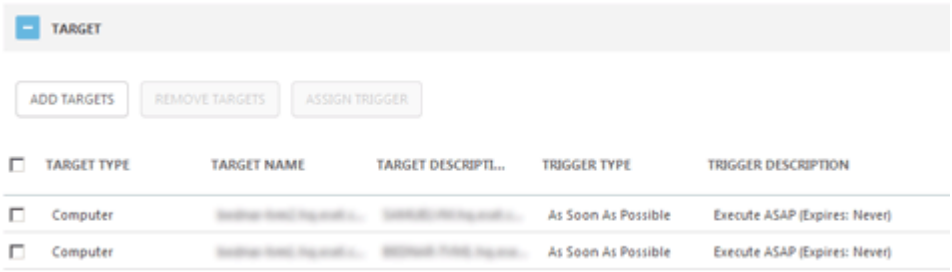
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.17 Anti-Theft Action

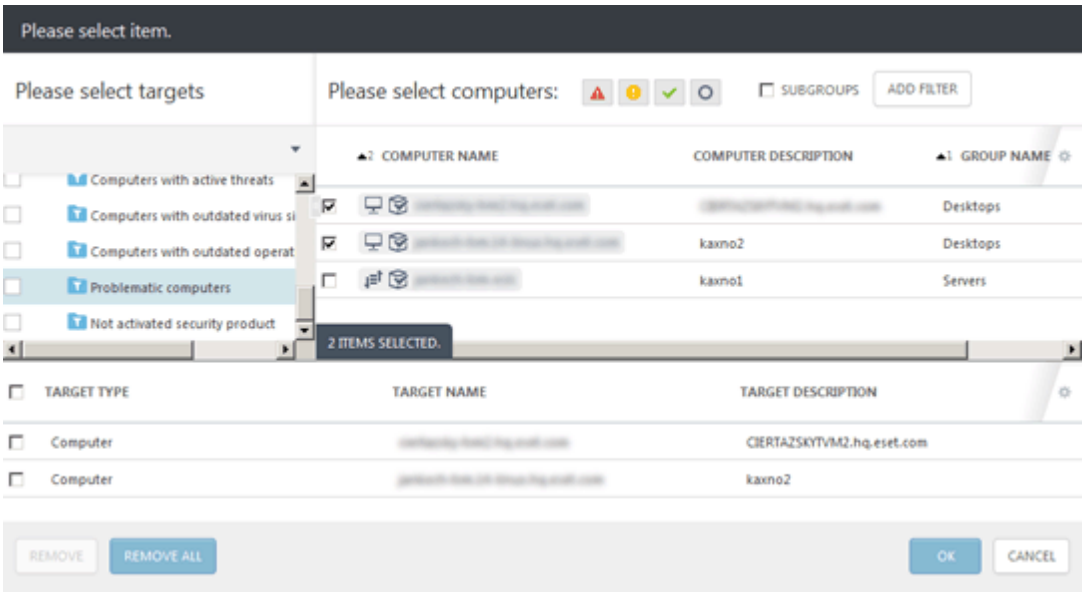
The **Anti-Theft** feature protects a mobile device from unauthorized access. If a mobile device (enrolled and managed by ERA) is lost or gets stolen, there are some actions that take place automatically and some actions can be performed using a client task. If an unauthorized person replaces a trusted SIM card with an untrusted SIM, the device will automatically be **locked** by ESET Endpoint Security for Android and an alert SMS will be sent to the user-defined phone number(s). This message will include the phone number of the SIM card currently in use, the **IMSI** (International Mobile Subscriber Identity) number and the phone's **IMEI** (International Mobile Equipment Identity) number. The unauthorized user will not be aware that this message has been sent because it will automatically be deleted from the device's messaging threads. You can also request the **GPS** coordinates of the lost mobile device or remotely erase all data stored on the device using a client task.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

- **Find** - The device will reply with a text message containing its GPS coordinates. If a more precise location is available after 10 minutes, the device will re-send the message.
- **Lock** - The device will be locked. The device can be unlocked using the admin password or the unlock command.
- **Unlock -** The device will be unlocked so it can be used again. The SIM card currently in the device will be saved as a Trusted SIM.
- **Siren -** The device will be locked and it will play a very loud sound for 5 minutes (or until unlocked).
- **Wipe -** All accessible data on the device will be erased (files will be overwritten). ESET Endpoint Security will remain on the device. This can take up to several hours.
- **Enhanced Factory Reset** - All accessible data on the device will be erased (file headers will be destroyed) and the device will be reset to its default factory settings. This can take several minutes.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.2.18 Device Enrollment

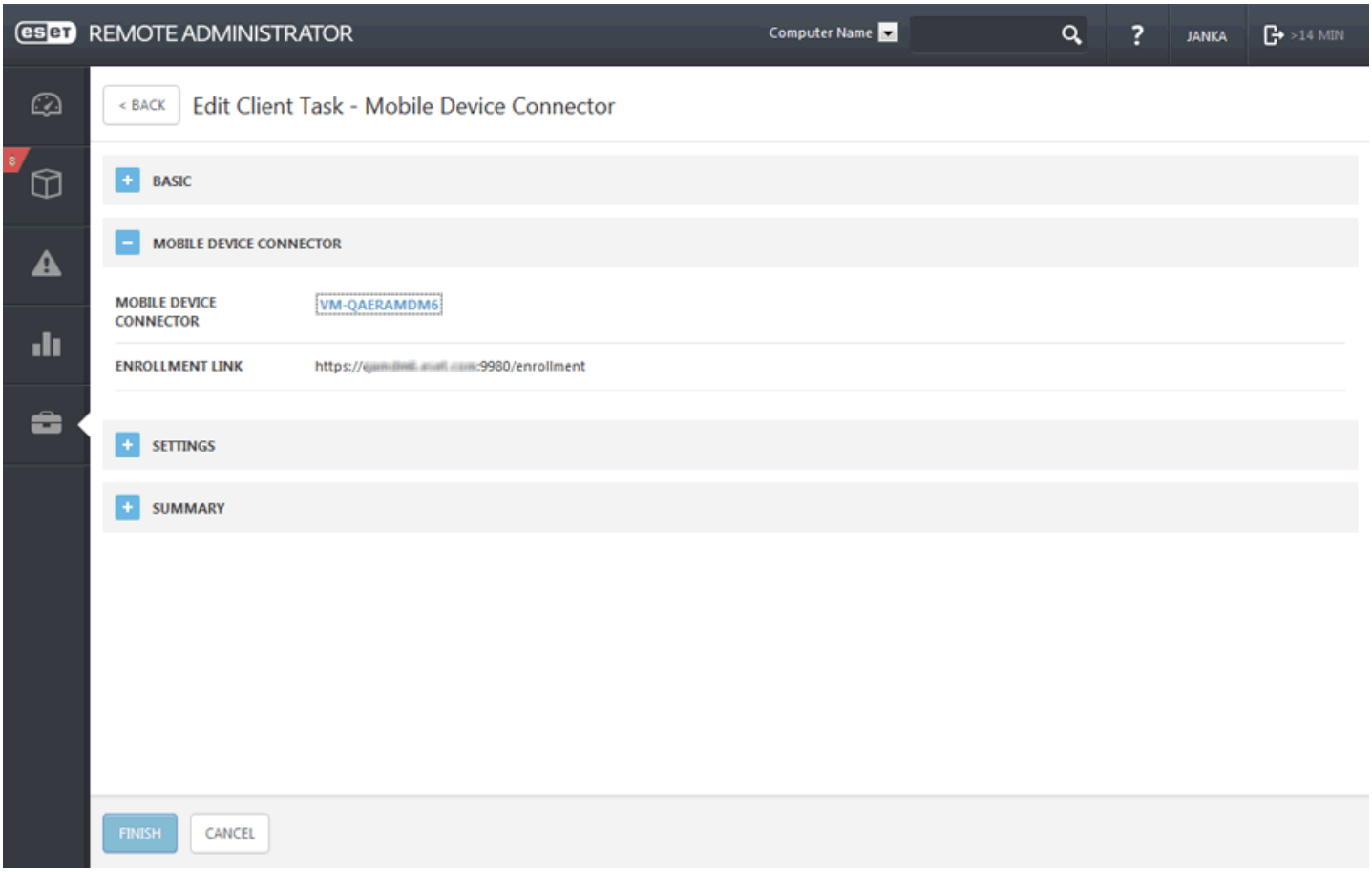
Mobile phones can be managed by the ERA Server using the ESET Endpoint Security for Android version 2 mobile app. To start managing mobile devices, you need to enroll them into ERA. Device Enrollment is done using a Client task.

Basic

Enter task **Name** and **Description** (optional).

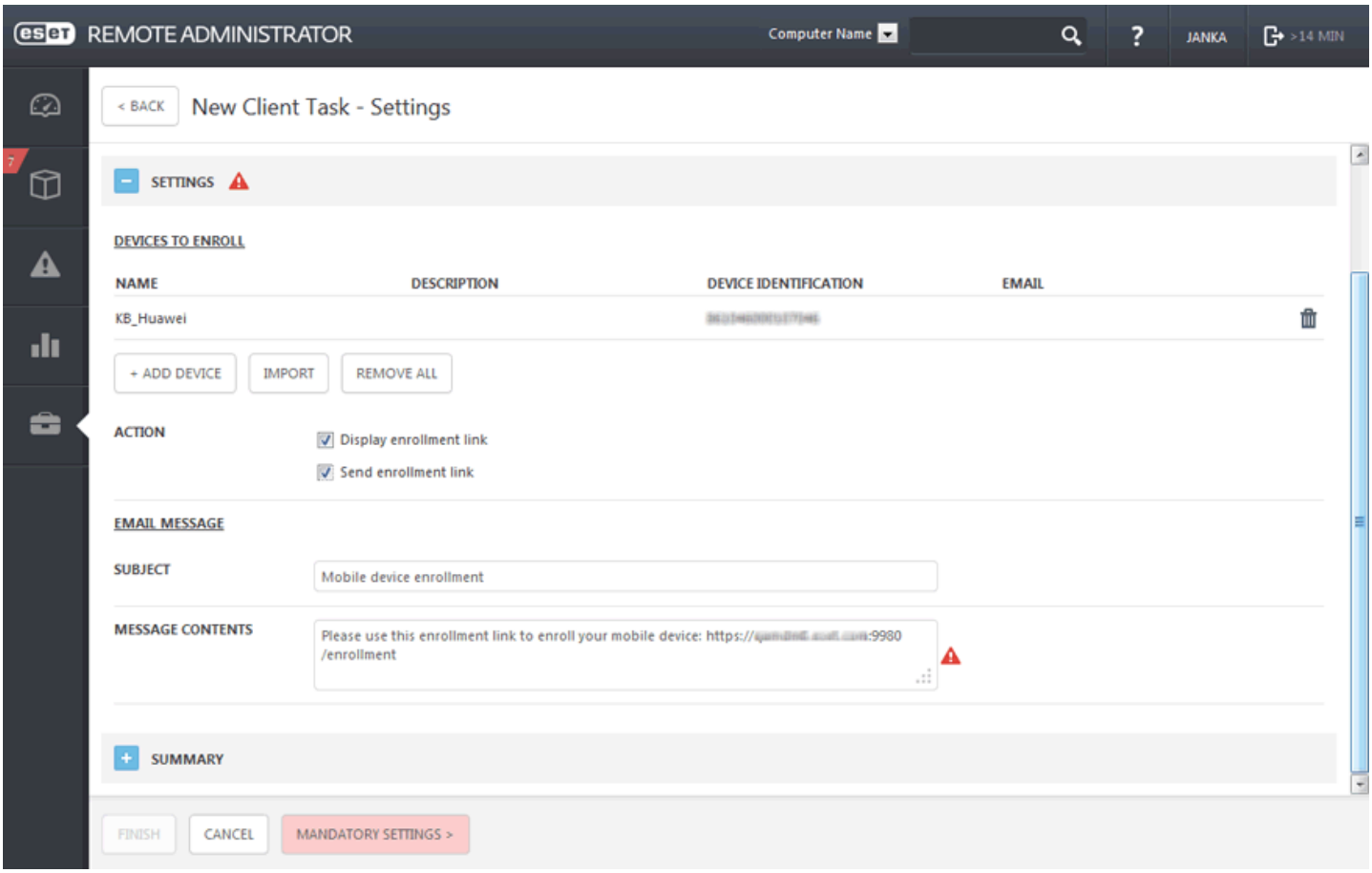
Mobile Device Connector

Select the machine where Mobile Device Connector is installed. An enrollment link (URL) will be displayed automatically. If no links are displayed after clicking **Select**, make sure that the Mobile Device Connector server is accessible. If you do not have Mobile Device Connector installed yet, refer to the Mobile Device Connector installation - Windows or Linux chapters of this guide for installation instructions.



Settings

Type the **Name** of the mobile device (this name will be shown in the list of Computers), and optionally a **Description**. Enter the IMEI number for the particular mobile device you want to add. We also recommend that you enter the **Email** address that is associated with the mobile device (the enrollment link will be sent to this email address). Click **+ Add device** if you want to add another mobile device, you can add multiple devices at the same time. Specify an **Action** by selecting the check box next to **Display enrollment link** and/or **Send enrollment link** (the URL will be sent to the email address(es) associated with the device). If you want to send an enrollment link (recommended) to the mobile device, you can edit the **Subject** and **Message contents**, but make sure to keep the enrollment URL unchanged.



Summary

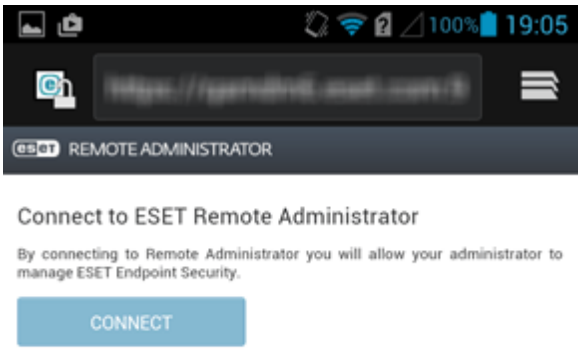
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

After you click **Finish**, the enrollment link (URL) will be displayed. If you do not specify an email address and did not select **Send enrollment link**, you must either type the URL into the web browser on the mobile device manually, or send this URL to the mobile device by other means.

There are two scenarios for enrollment, when ESET Endpoint Security for Android (EESA) is activated on the mobile device. You'll activate EESA on the mobile device using ERA Product Activation client task (recommended). The other scenario is for mobile devices with EESA app already activated.

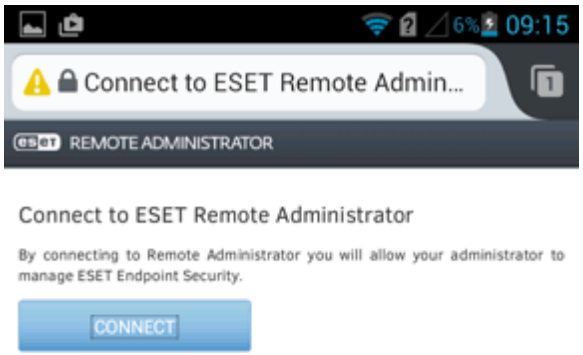
EESA not activated yet - follow the steps below to activate product and enroll your Device:

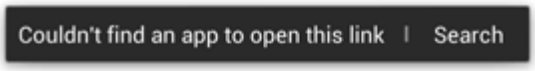
1. Tap the enrollment link URL received via email, or type it into the browser manually, including the port number (for example, *https://eramdm:9980/enrollment*). You might be asked to accept an SSL certificate, click **accept** if you agree and then click **Connect**.


19:05
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT

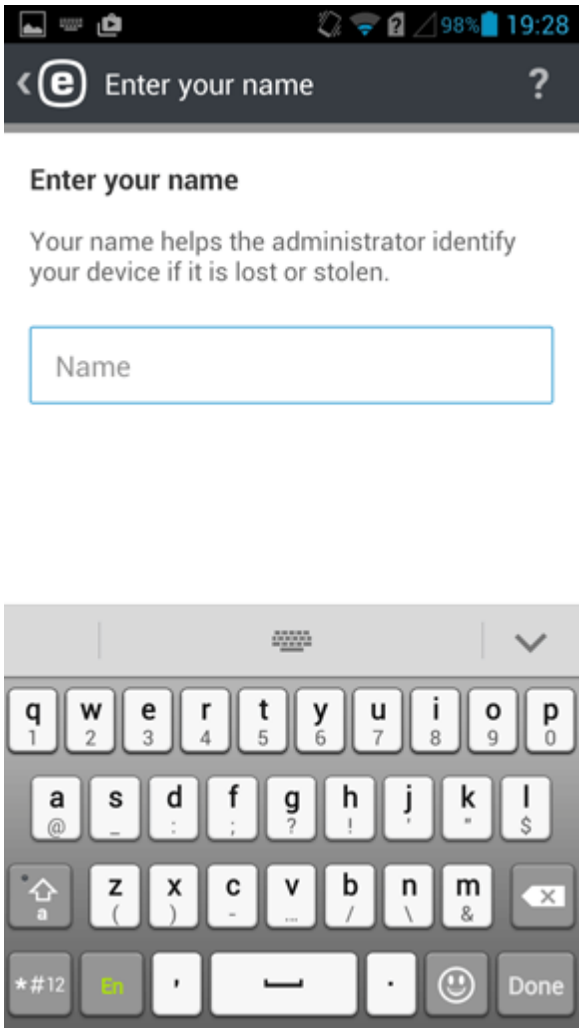
2. If you do not have ESET Endpoint Security installed on the mobile device, you will automatically be redirected to the Google Play store, where you can download the app.

NOTE: If you receive the notification **Couldn't find an app to open this link**, try opening the enrollment link in the default Android web browser.

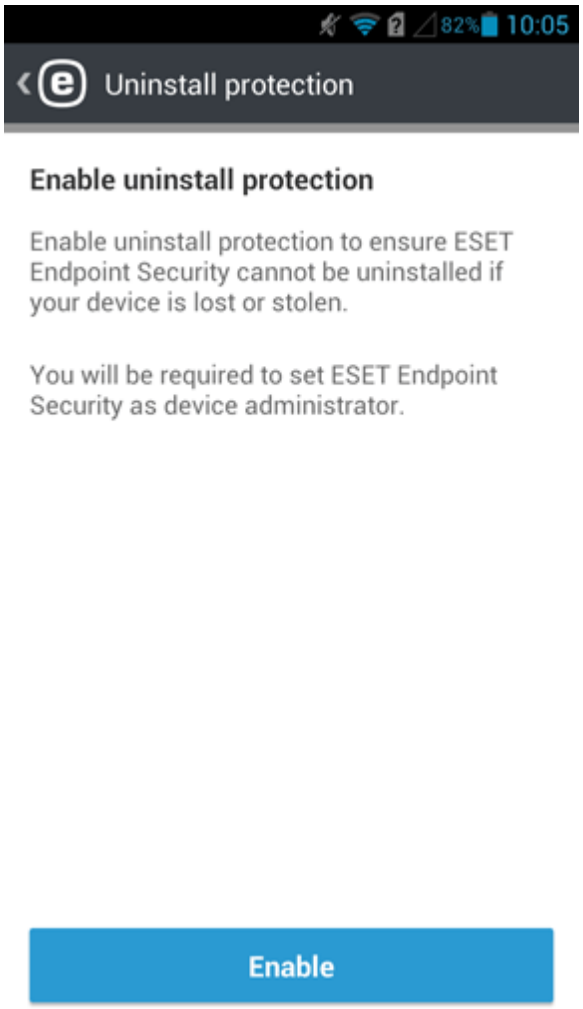

09:15
Connect to ESET Remote Admin...
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT



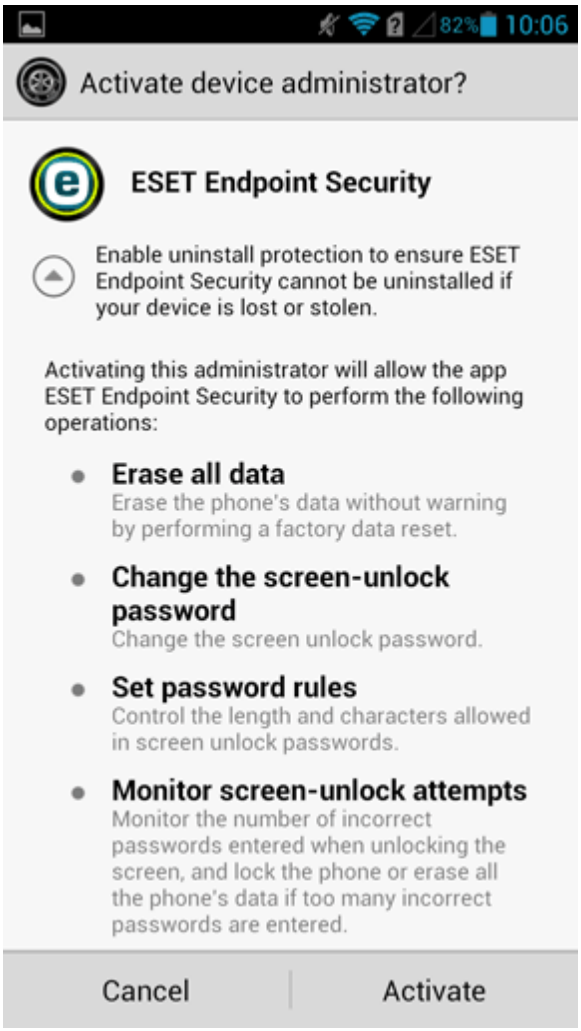
3. Enter the name of the mobile device user.


98% 19:28
Enter your name
Enter your name
Your name helps the administrator identify your device if it is lost or stolen.
Name
Done

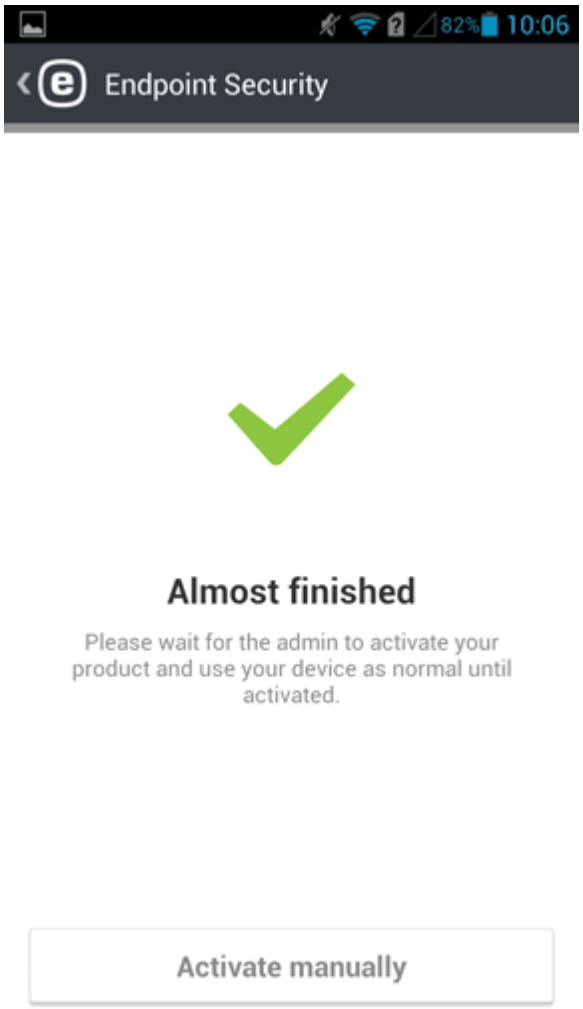
4. Tap **Enable** to enable uninstall protection.


82% 10:05
Uninstall protection
Enable uninstall protection
Enable uninstall protection to ensure ESET Endpoint Security cannot be uninstalled if your device is lost or stolen.
You will be required to set ESET Endpoint Security as device administrator.
Enable

5. Tap **Activate** to activate device administrator.

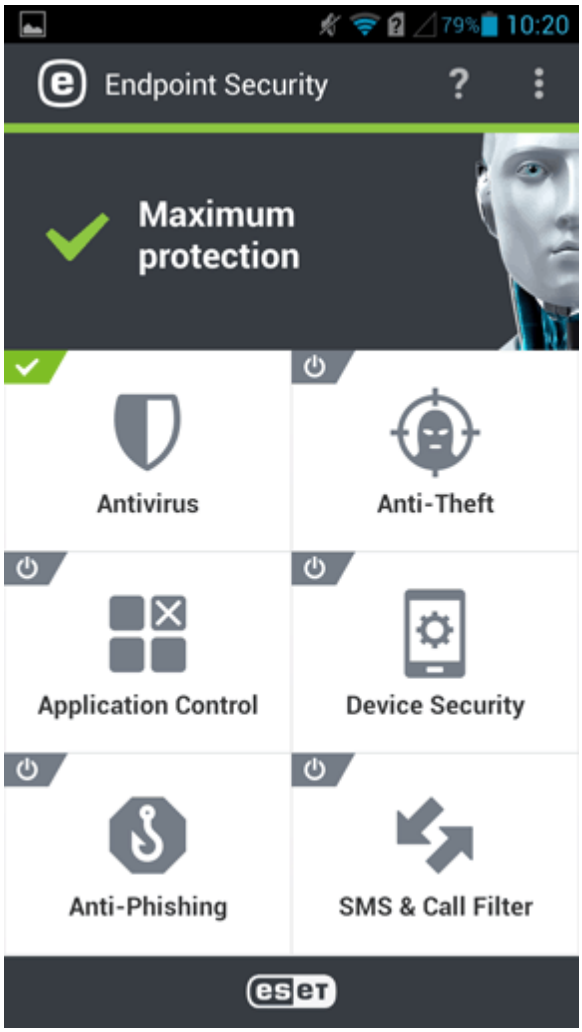

82% 10:06
Activate device administrator?
ESET Endpoint Security
Enable uninstall protection to ensure ESET Endpoint Security cannot be uninstalled if your device is lost or stolen.
Activating this administrator will allow the app ESET Endpoint Security to perform the following operations:
Erase all data
Erase the phone's data without warning by performing a factory data reset.
Change the screen-unlock password
Change the screen unlock password.
Set password rules
Control the length and characters allowed in screen unlock passwords.
Monitor screen-unlock attempts
Monitor the number of incorrect passwords entered when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are entered.
Cancel
Activate

6. At this point, you can exit the EESA app on the mobile device and open ERA Web Console.


82% 10:06
Endpoint Security
Almost finished
Please wait for the admin to activate your product and use your device as normal until activated.
Activate manually

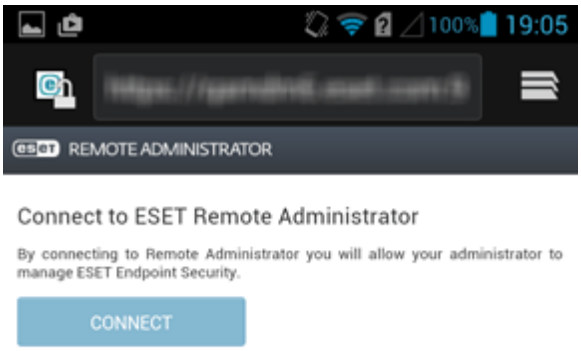
7. In ERA Web Console, go to **Admin** > **Client Tasks** > **Mobile** > Product Activation and click **New**.
8. Select the mobile device by clicking **Add targets**.
9. Under Settings, click <Choose ESET license> and select appropriate license. Click **Finish**.

It might take some time for the Product Activation client task to run on the mobile device. Once the task is successfully executed, the EESA app is activated and the mobile device is being managed by ERA. The user will now be able use the EESA app. When the EESA app is open, main menu is displayed:



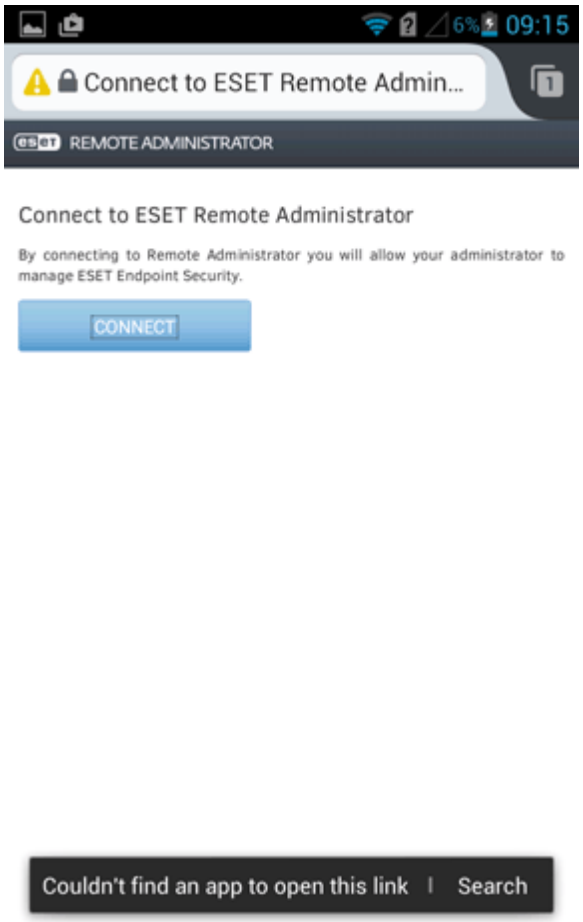
EESA already activated - follow the steps below to enroll your Device:

1. Tap the enrollment link URL received via email, or type it into the browser manually, including the port number (for example, *https://eramdm:9980*). You might be asked to accept an SSL certificate, click **accept** if you agree and then click **Connect**.

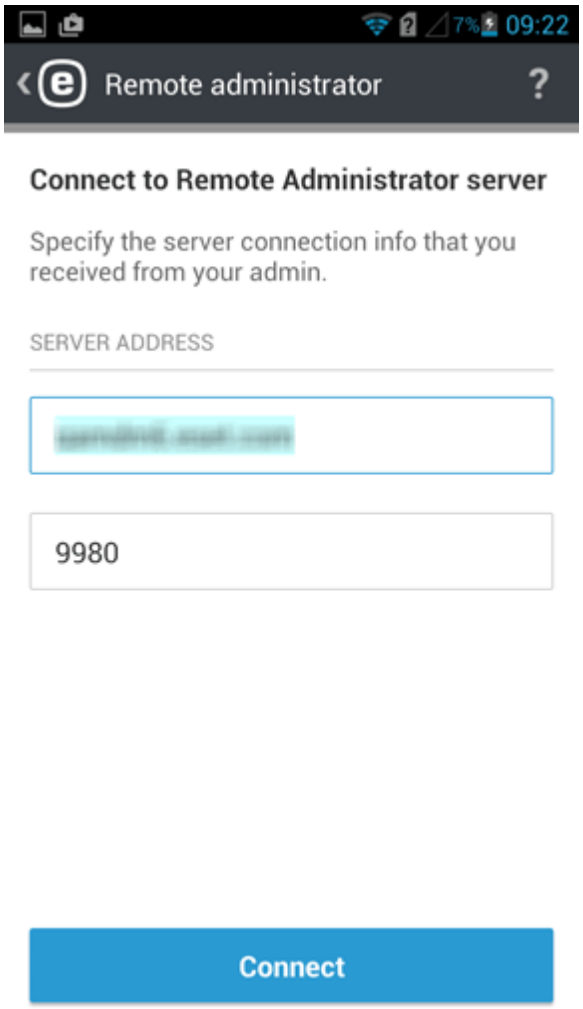

100% 19:05
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT

NOTE: If you do not have ESET Endpoint Security installed on the mobile device, you will automatically be redirected to the Google Play store, where you can download the app.

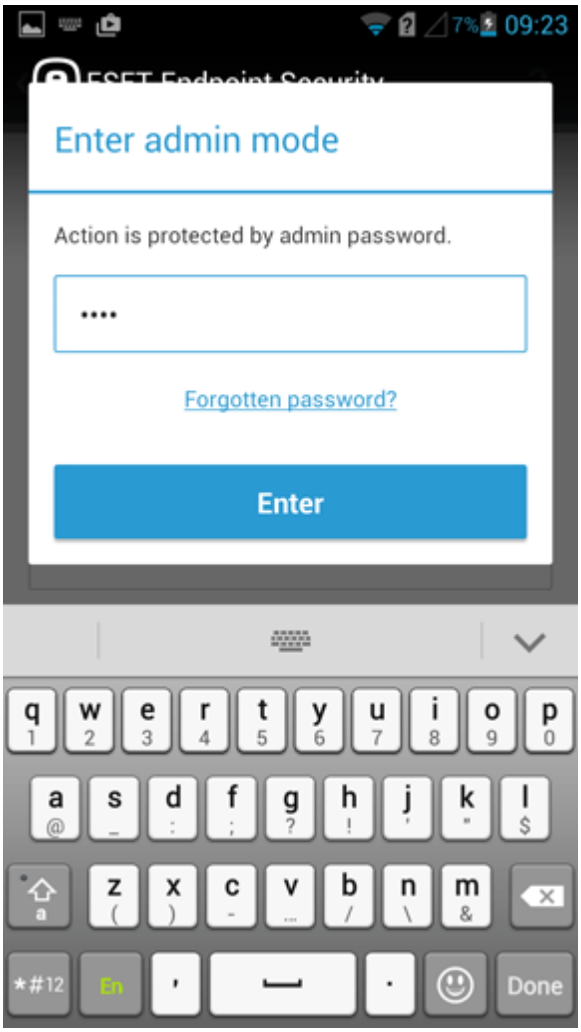
NOTE: If you receive the notification **Couldn't find an app to open this link**, try opening the enrollment link in the default Android web browser.


09:15
Connect to ESET Remote Admin...
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT
Couldn't find an app to open this link
Search

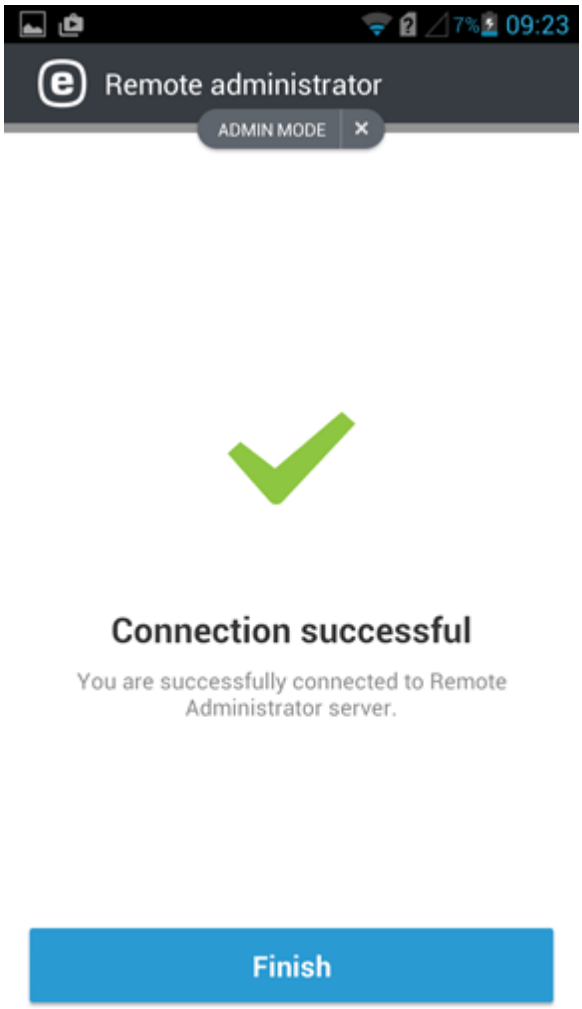
2. Check your connection details (Mobile Device Connector server address and port) and click **Connect**.



3. Type the ESET Endpoint Security admin mode password into the blank field and tap **Enter**.



4. This mobile device is now being managed by ERA, tap **Finish**.



6.1.3.2.19 Stop Managing (Uninstall ERA Agent)

- **Desktop** - This task will remove the Agent installed on the machine where MDM is installed.
- **Mobile** - This task will cancel MDM enrollment of your mobile device.

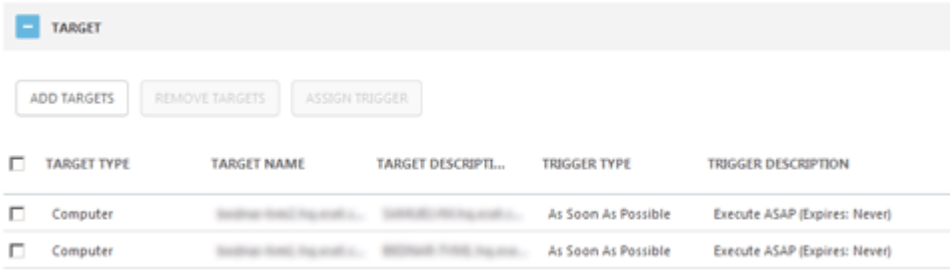
After the device is no longer managed (Agent is removed), some settings may remain in the managed products. We recommend that you reset some settings (for example, password protection) to default settings using a policy before the device is removed from management. Also, all tasks running on the Agent will be abandoned. The **Running**, **Finished** or **Failed** execution status of this task may not be displayed accurately in ERA Web Console depending on replication.

1. If the device has some special settings that you do not want to maintain, set a device policy that returns unwanted settings to default values (or values which are desirable).
2. Before performing this step, we recommend that you to wait long enough to be certain that policies from point 1 have finished replication on the target computer before deleting the computer from the list in ERA.
3. Before performing this step, we recommend that you to wait long enough to be certain that policies from point 2 have finished replication on the target computer.

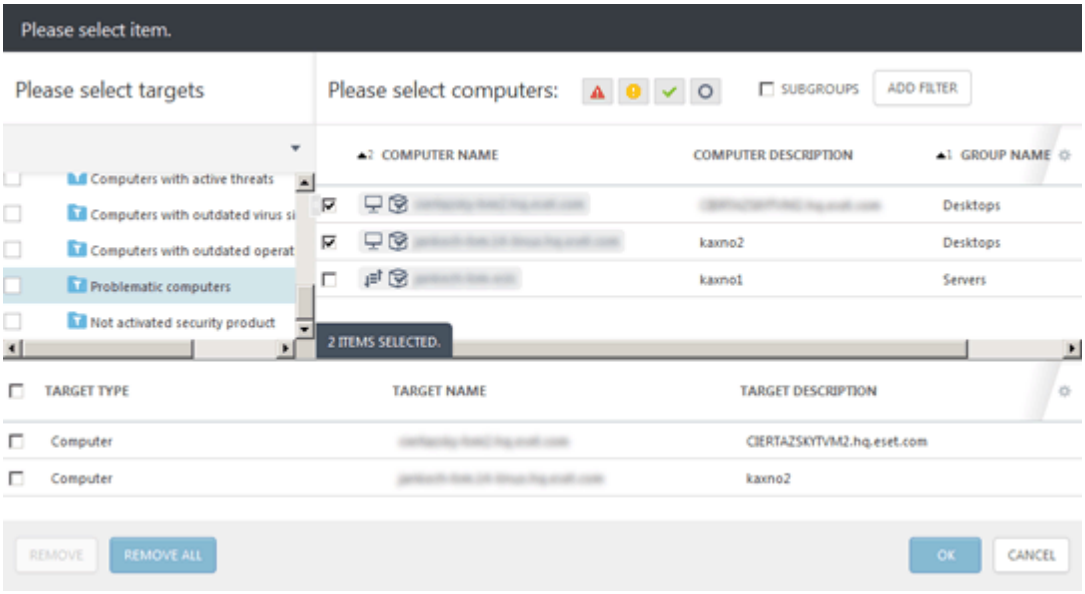
NOTE: Settings are not available for this task.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Summary

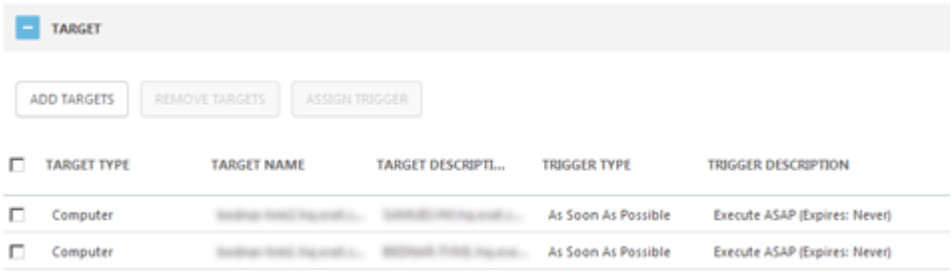
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.3 Export Managed Products Configuration

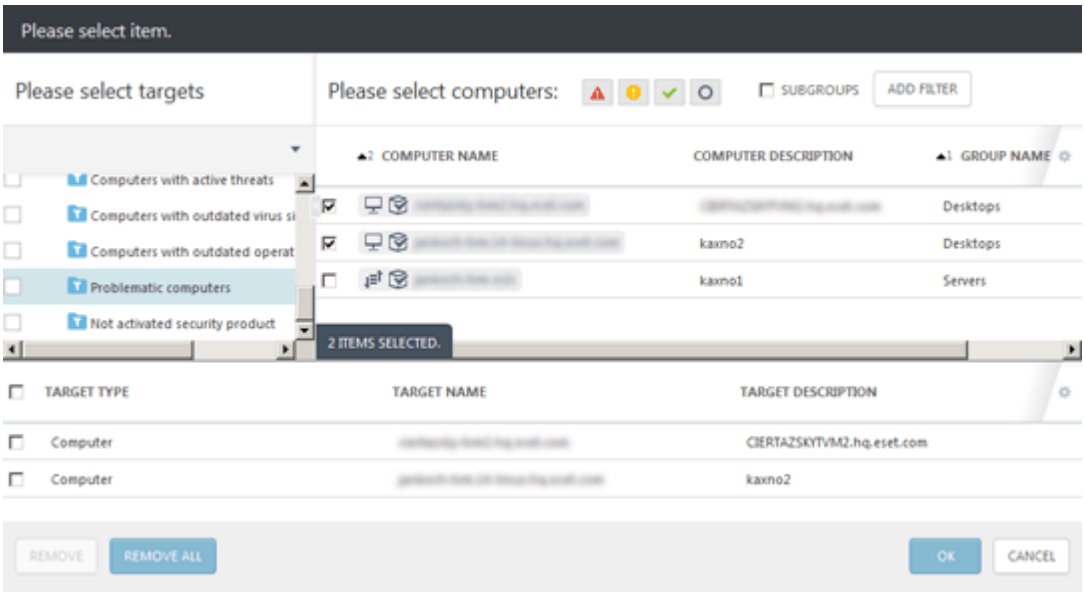
The **Export Managed Products Configuration** task is used to export the settings of individual ERA components or ESET security products installed on the client(s).

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Settings

Export managed products configuration settings

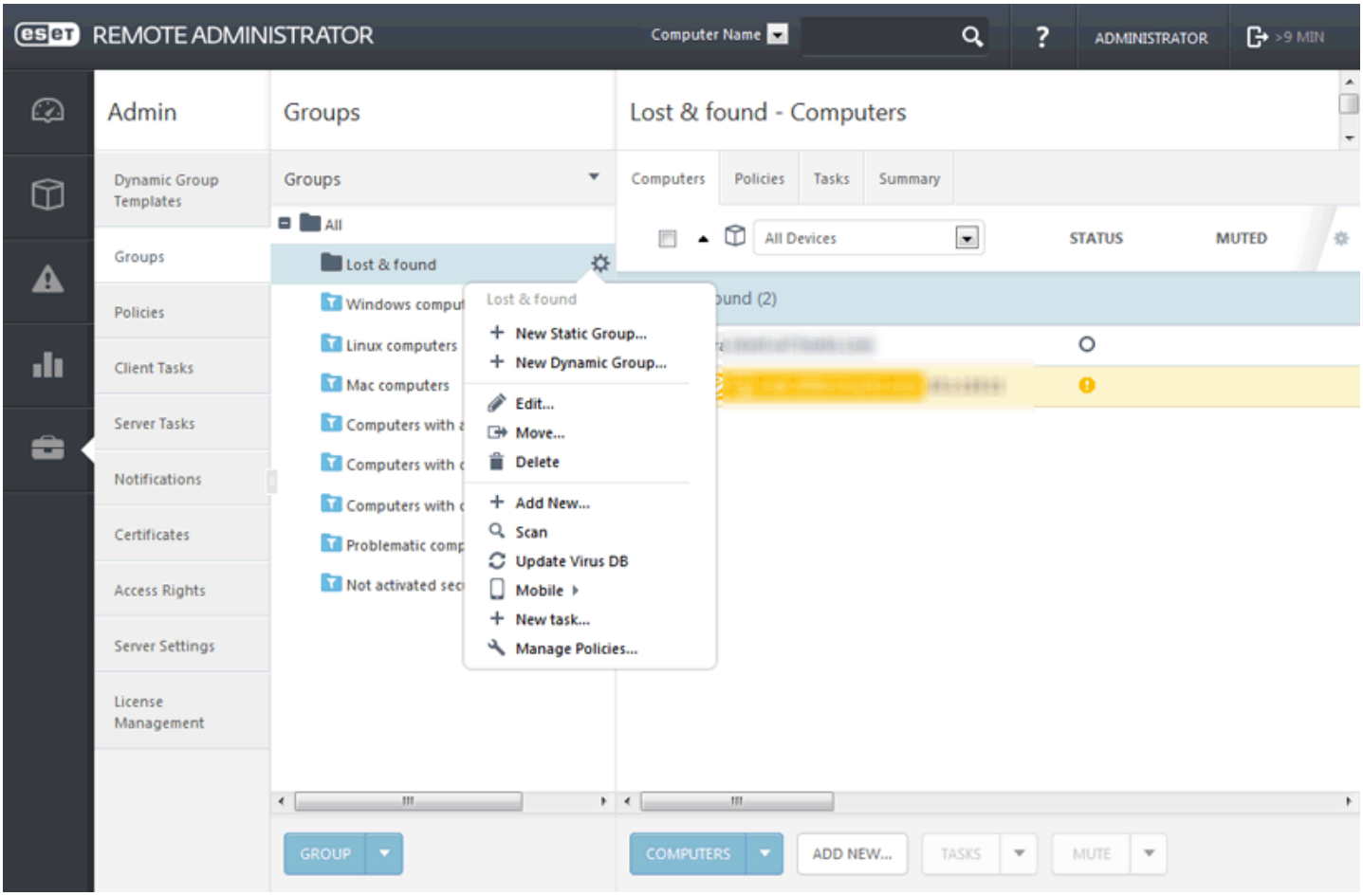
- **Product** - Select an ERA component or a client security product for which you want to export the configuration.

Summary

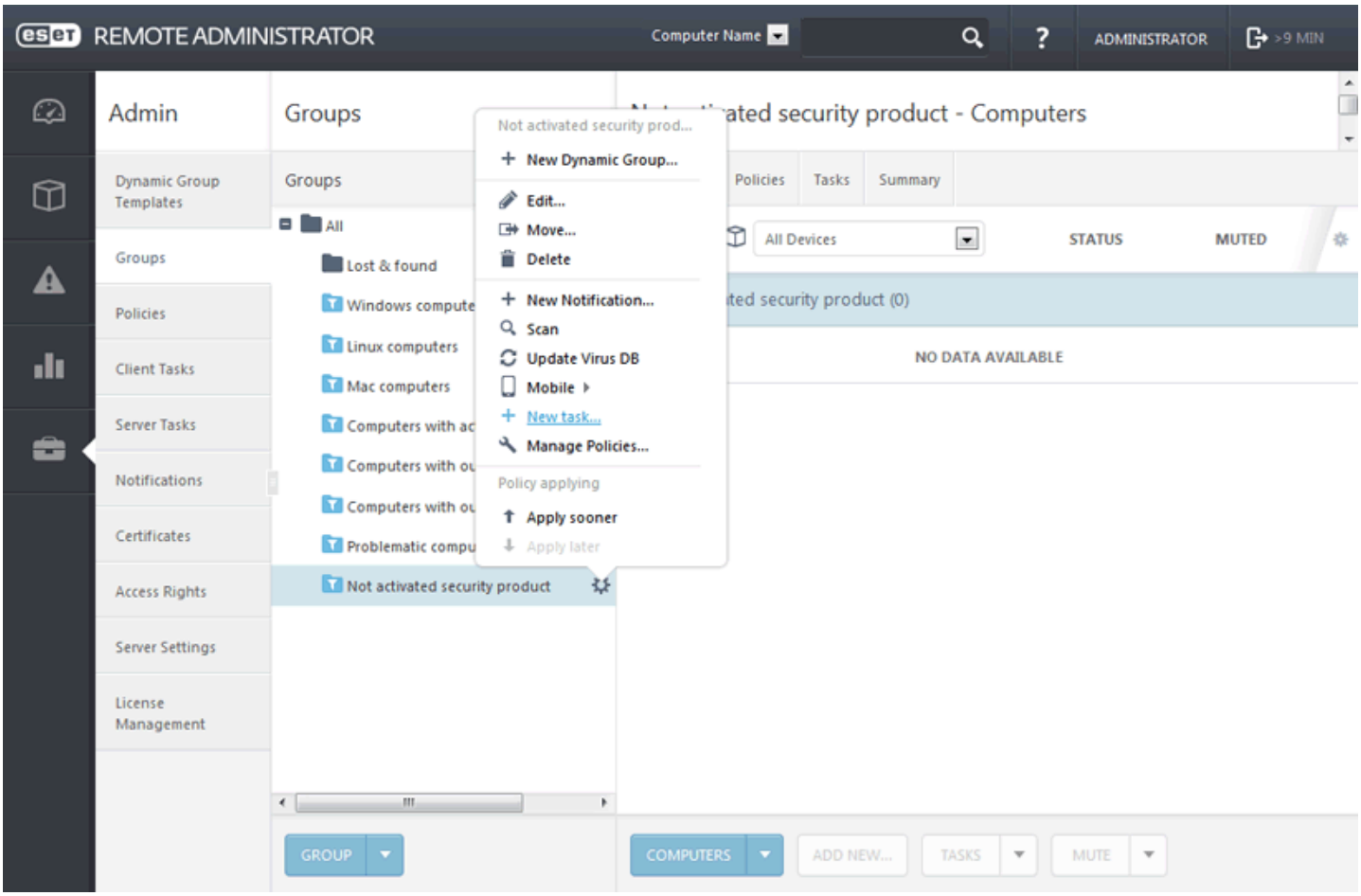
All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.1.3.4 Assign Task to Group

Click **Admin** > **Groups** > select **Static** or **Dynamic** group > ⚙ next to the selected group, or click **Group** > **+ New task**



The same can be done from **Computers**, select **Static** or **Dynamic** and click ⚙ > **+ New task**

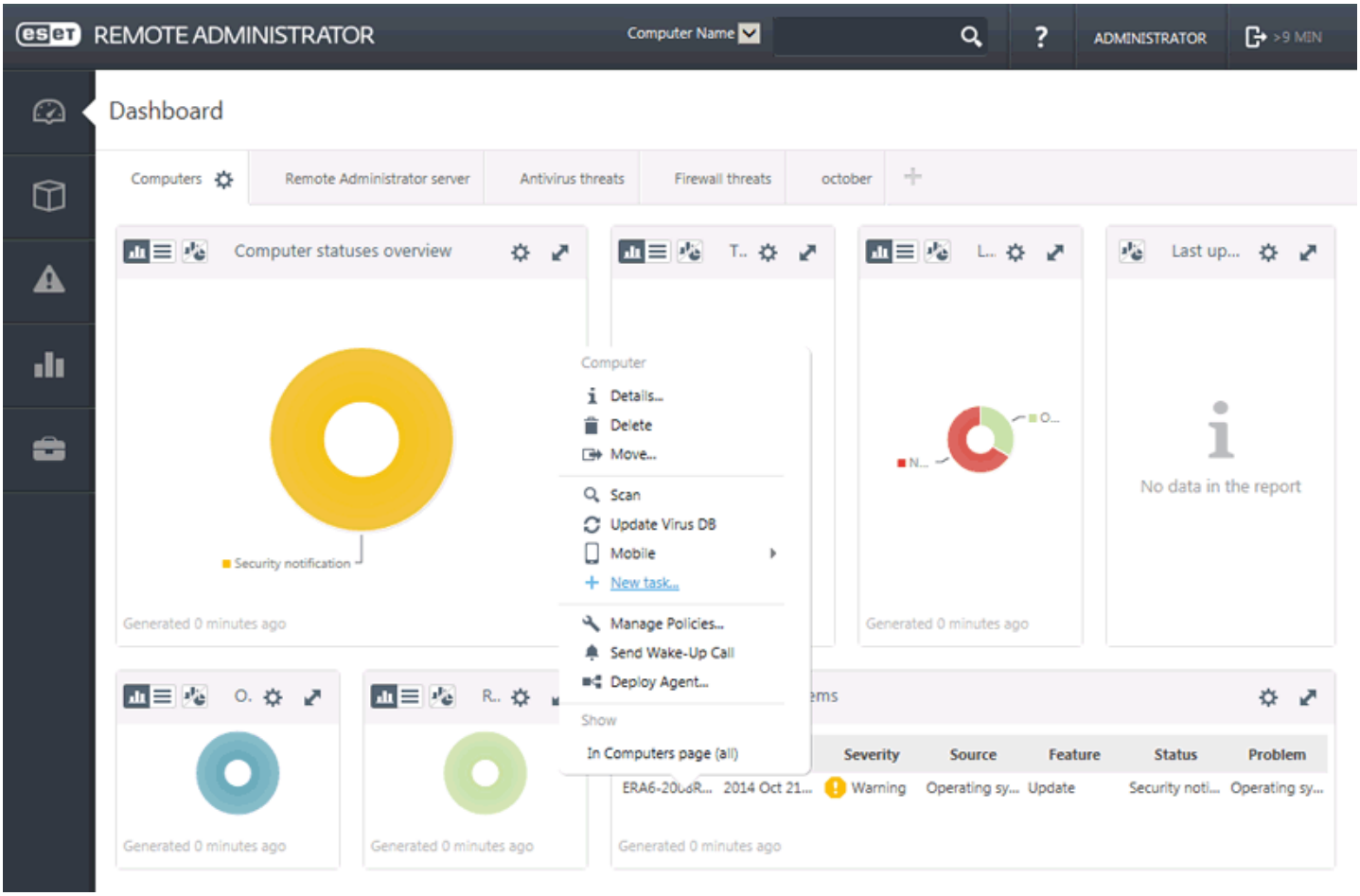


A New Client task wizard window will open.

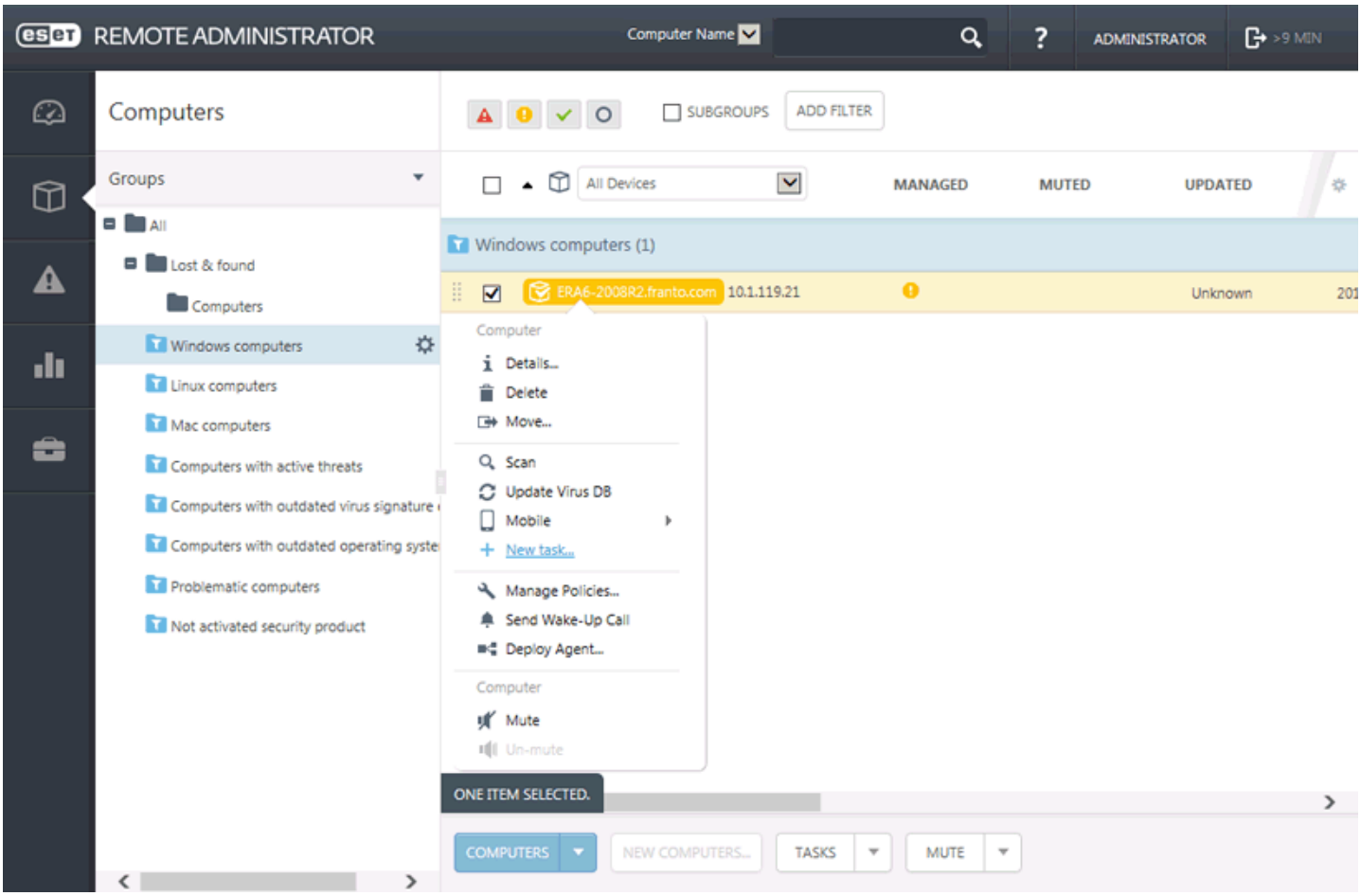
6.1.3.5 Assign Task to Computer(s)

There are three ways to assign a task to computer(s).

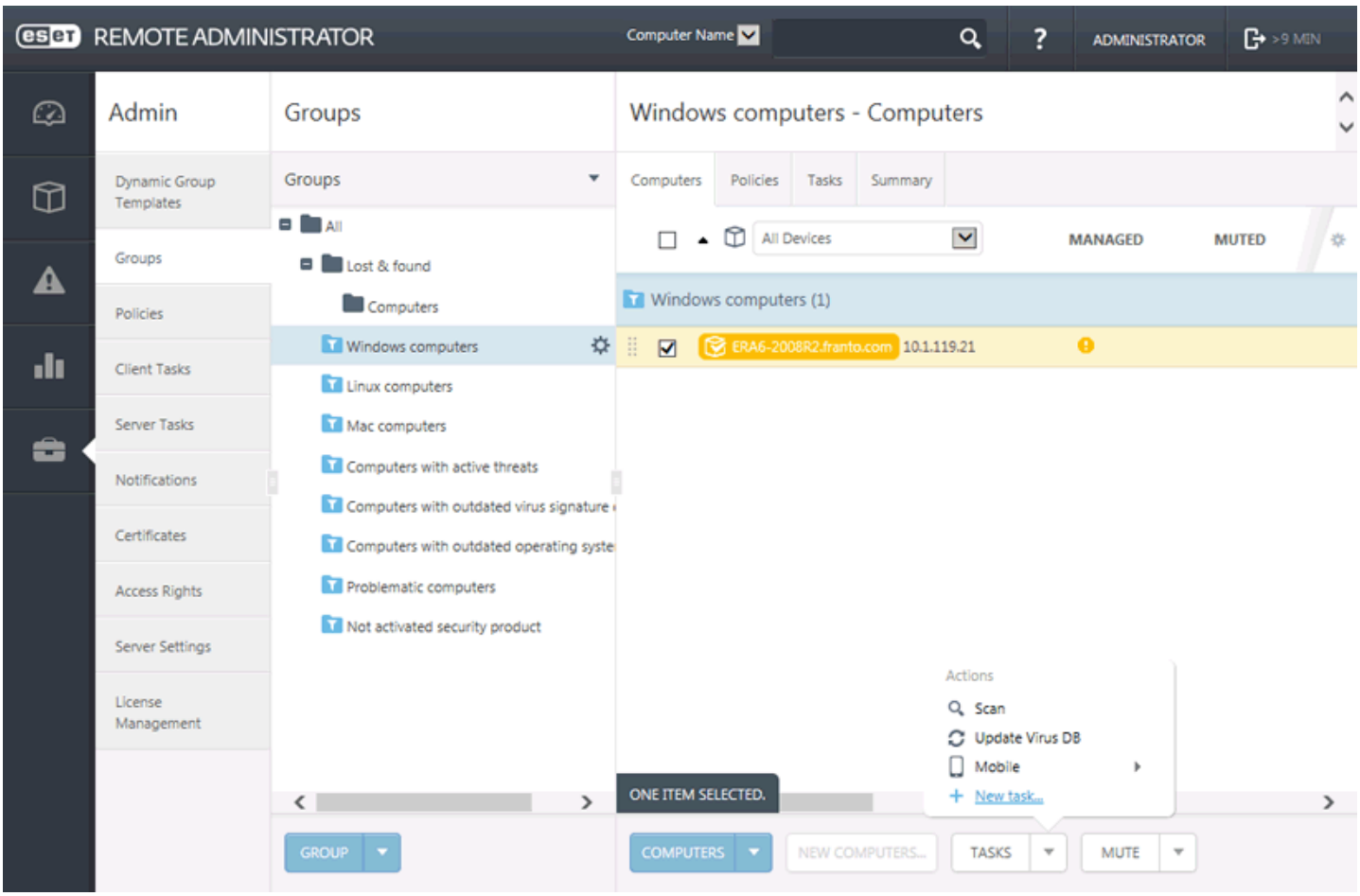
1. **Dashboard** > **Computers with problems** > select **+ New Task...**



2. **Computer** > select computer(s) using check boxes > select **+ New task...**



3. **Admin**> **Groups** > select computer(s) > **Tasks** button, select action and click **+ New task...**



A New Client task wizard window will open.

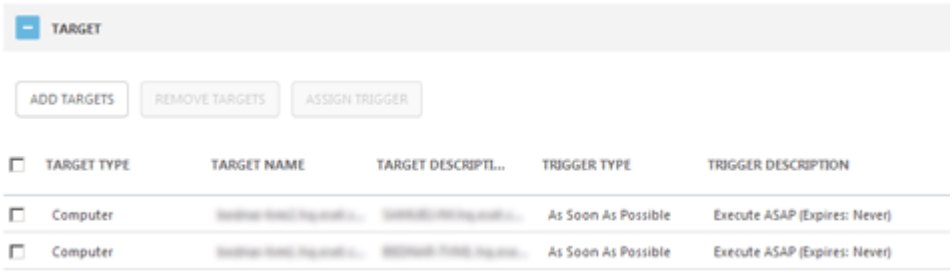
6.1.3.6 Schedule a Task

To create a scheduled task, do the following:

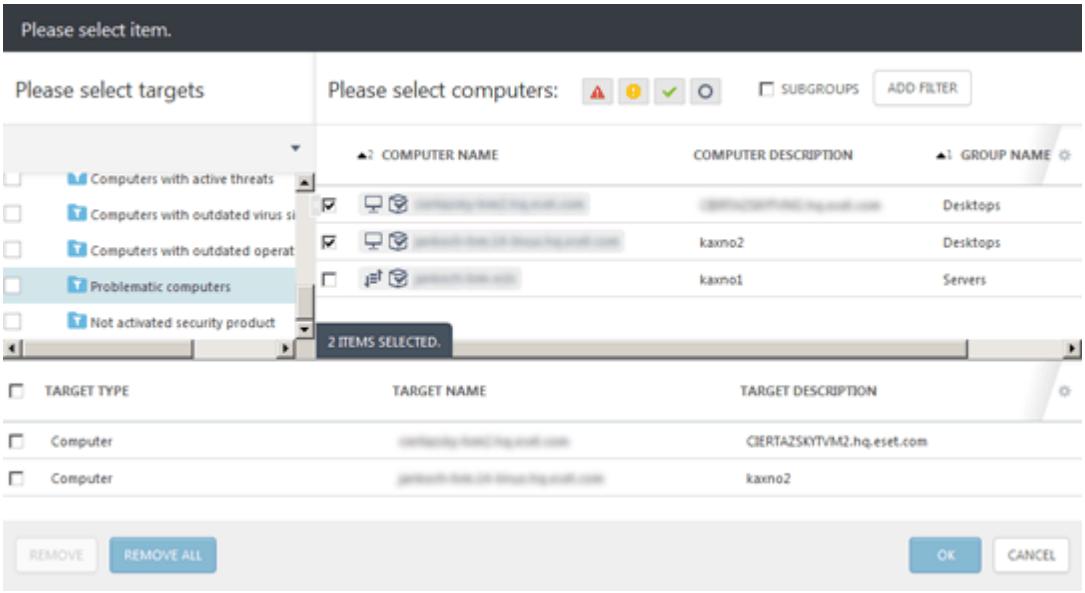
Navigate to **Admin** > **Client Tasks** > select **Task** and choose **Edit...** go to **Target**.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

6.1.3.7 Triggers

Triggers can be used on both the ERA Server and Agents (clients).

6.1.4 Server Tasks

Server Tasks can automate routine jobs. Server task can have Triggers configured, which means that the task will execute as soon as a certain combination of events occur on the ERA Server.

ERA Server can schedule any of the following tasks:

- Static Group Synchronization updates client information in groups so you work with current data.
- Agent Deployment distributes the Agent to client computers.
- Generate Report is used to generate reports on the go as they are needed.

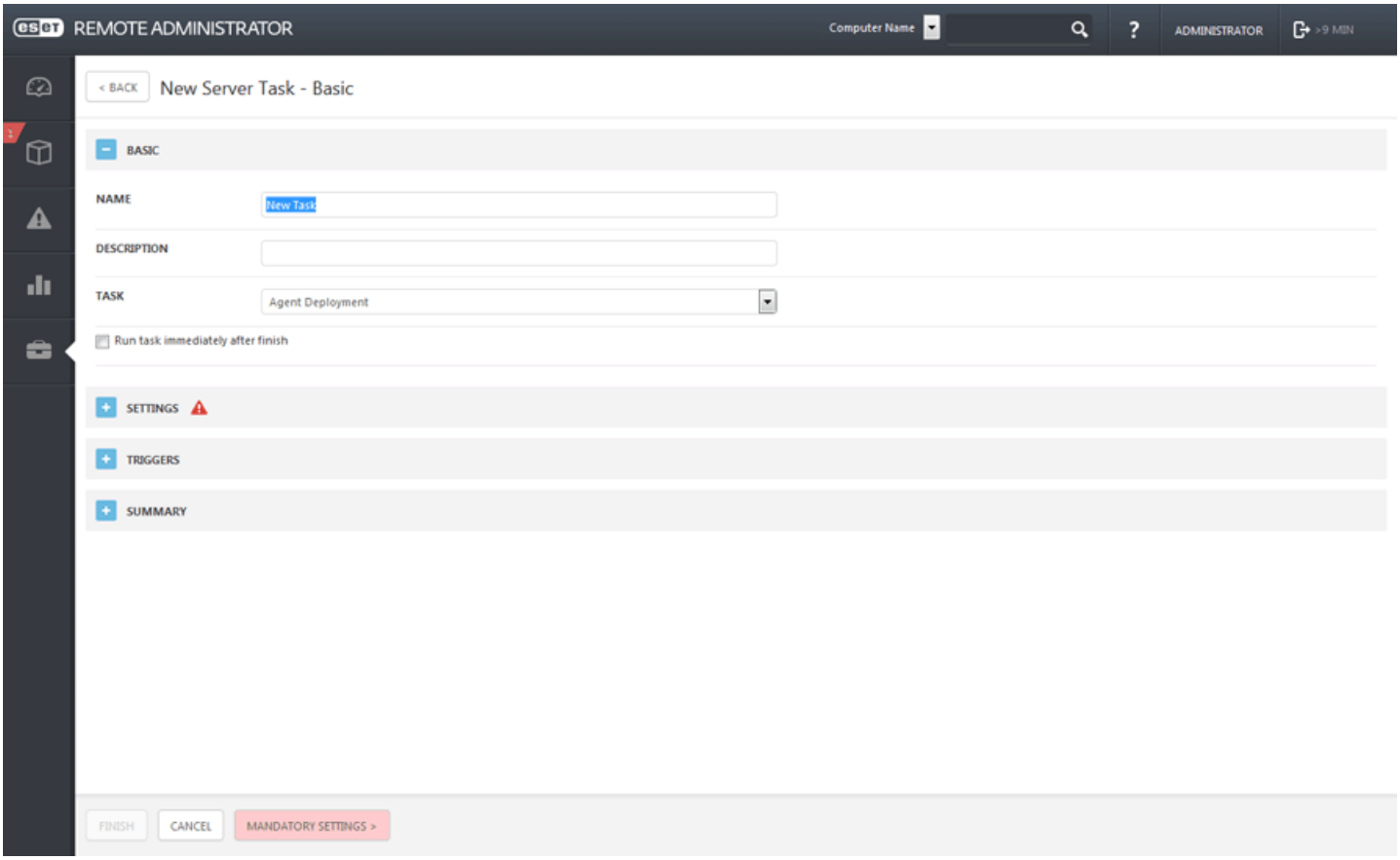
NOTE: Server Tasks cannot be assigned to any specific client or client group.

6.1.4.1 Server Task Wizard

To start creating your new task, click **Admin** > **Server Tasks** > **New**.

Basic

Enter basic information about the task, such as a **Name**, **Description** (optional) and the **Task Type**. The **Task Type** defines the settings and the behavior of the task. Select the check box next to **Run task immediately after finish** to have the task run automatically after you click **Finish**.



6.1.4.2 Manage Server Tasks

The following Server Tasks are pre-defined:

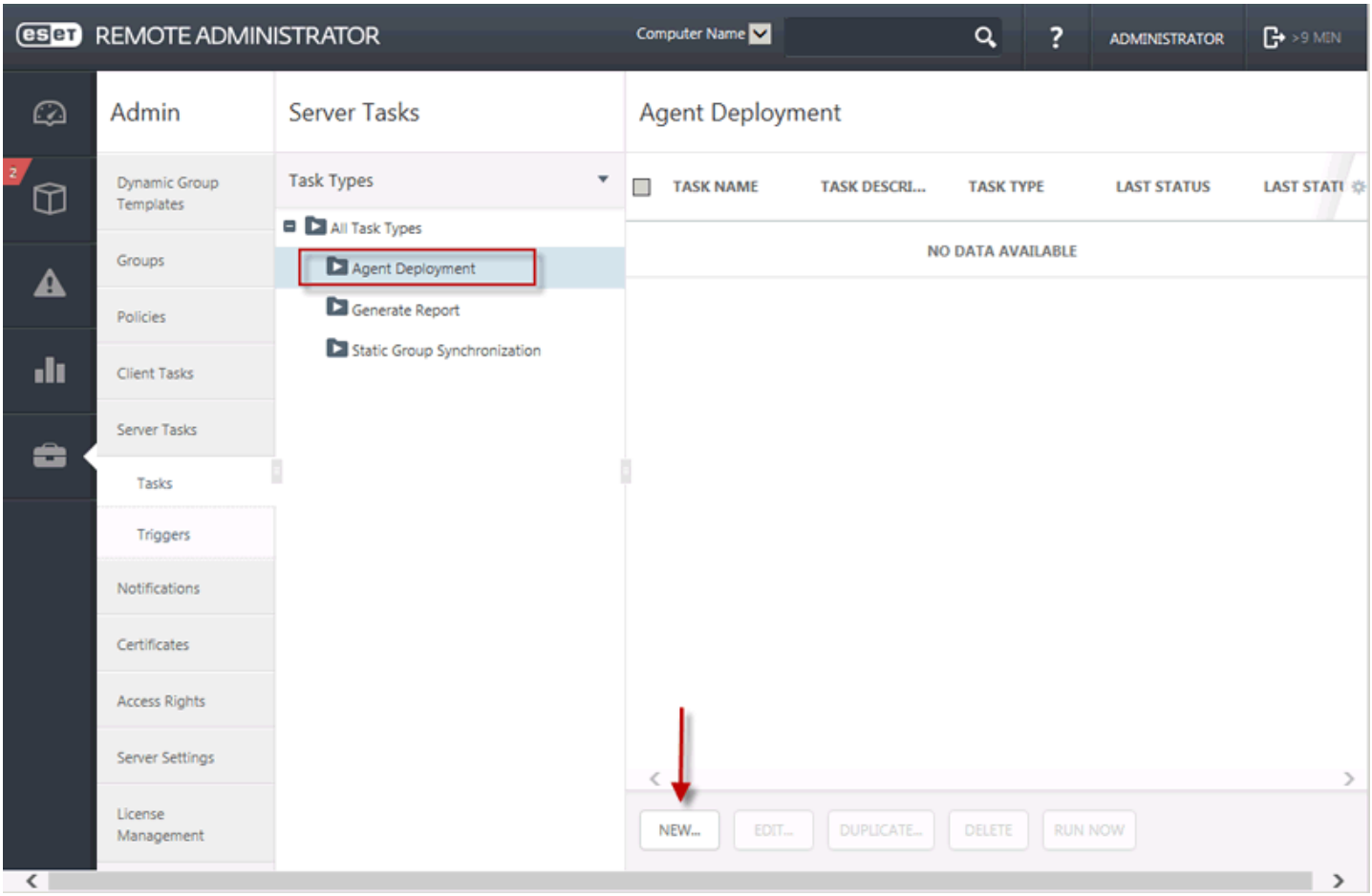
- Static Group Synchronization updates group information to display current data.
- Agent Deployment distributes the Agent to client computers.
- Generate Report is used to generate reports as they are needed.

6.1.4.2.1 Agent Deployment

Remote deployment of the ERA Agent is performed from the **Admin** section. Use following written instructions or watch Knowledgebase instructional video.

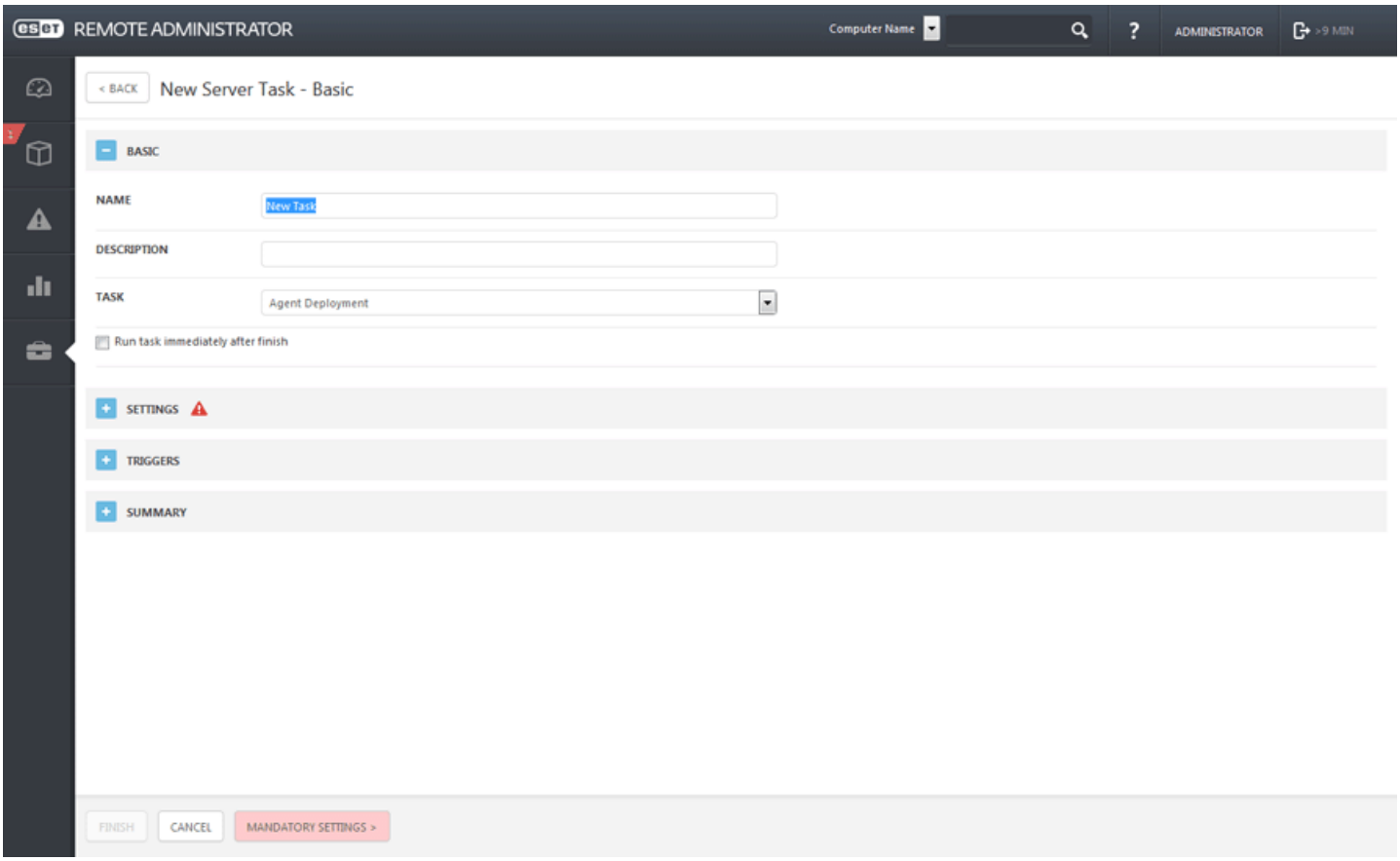
NOTE: We recommend you to first test mass Agent deployment in your environment. Once it's working fine, then you can begin with actual deployment on users client computers. Also, before you start testing mass deployment, change Agent connection interval.

Click **Server Task** > **Agent Deployment** > **New...** to start configuring your new task.



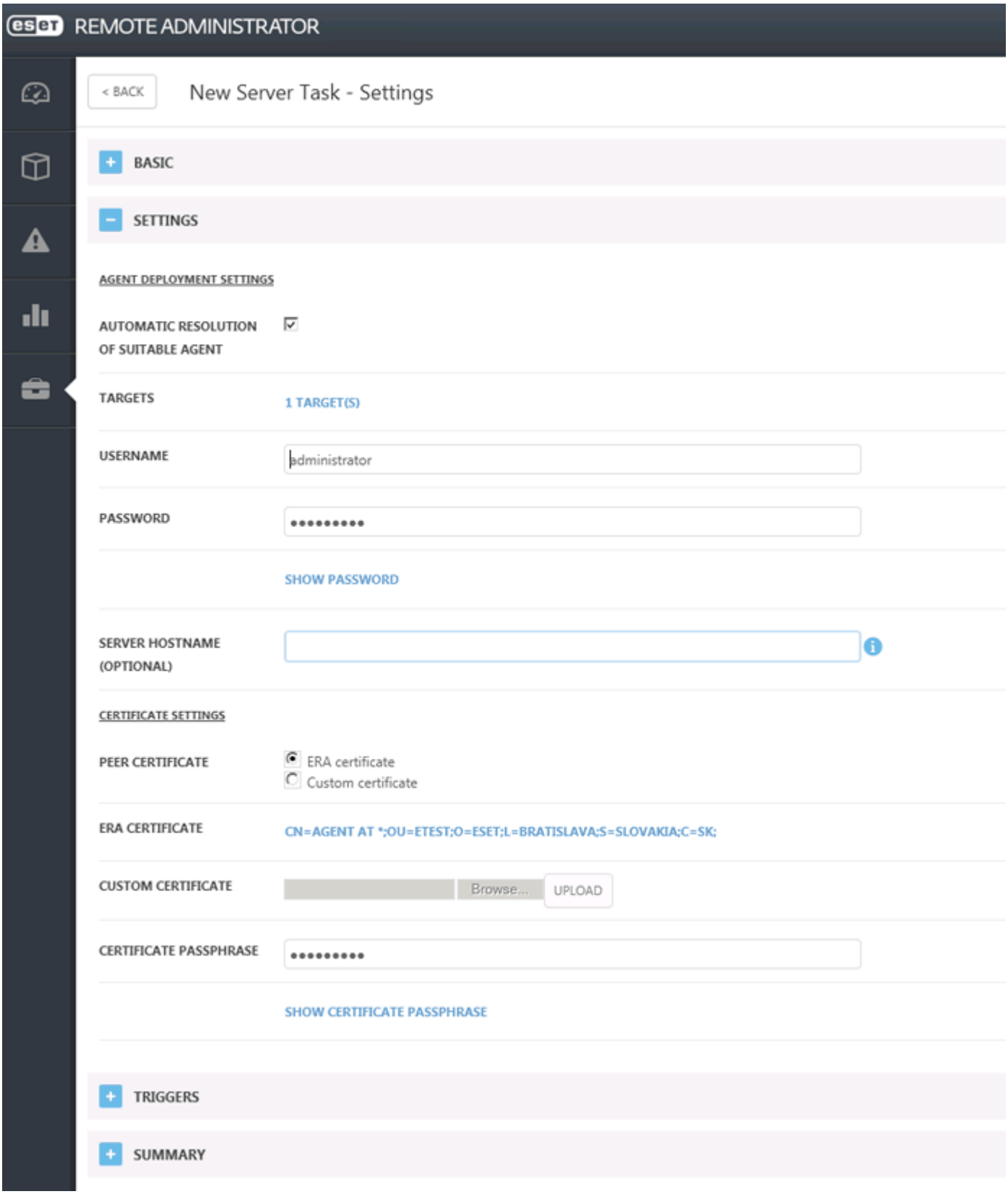
Basic

Enter basic information about the task, such as the **Name**, **Description** (optional) and **Task Type**. The **Task Type** defines the settings and behavior of the task. Select the check box next to **Run task immediately after finish** to have the task run automatically after you click **Finish**.



Settings

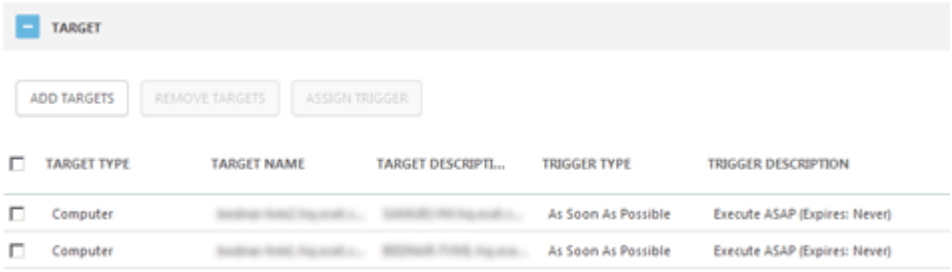
- **Automatic resolution of suitable Agent** - If you have multiple operating systems (Windows, Linux, Mac OS) in your network, select this option and this task will automatically find the appropriate server-compatible Agent installation package for each system.
- **Targets** - Click this to select the clients that will be the recipients of this task.
- **Username/Password** - The username and the password for the user with sufficient rights to perform a remote installation of the agent.
- **Server hostname (optional)** - You can enter a server hostname if it is different on the client side and the server side.
- **Peer certificate/ERA Certificate** - This is the security certificate and certificate authority for the agent installation. You can select the default certificate and certificate authority, or use custom certificates. For more information, see the Certificates chapter.
- **Custom certificate** - If you use a custom certificate for authentication, navigate to the certificate and select it when installing the Agent.
- **Certificate passphrase** - Password for the certificate, either the password you entered during Server installation (in the step where you created a certificate authority) or the password for your custom certificate.



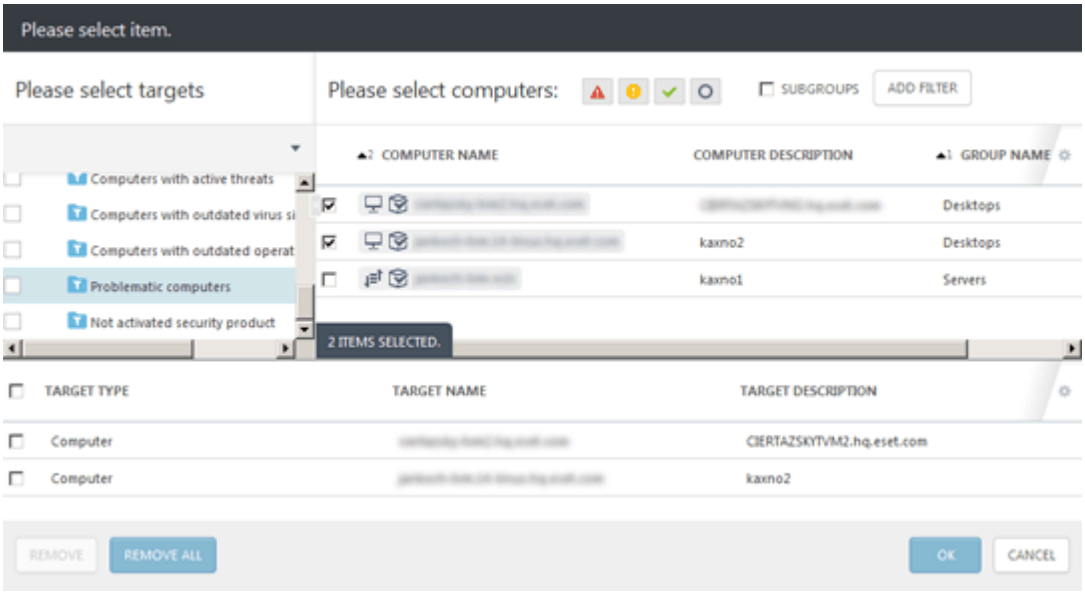
NOTE: ERA Server can select the appropriate Agent installation package for operating systems automatically. To choose a package manually, deselect **Automatic resolution of suitable Agent** and then choose the package you want to use from the list of available Agents in ERA repository.

Target

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.



Click **Add targets** to display all static and Dynamic Groups and their members.



Select clients, click **OK** and proceed to the **Trigger** section.

Trigger - Determines what event triggers the task.

- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON Expression.
- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the **Expiration date**, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the **log type**, **logical operator** and **filtering** criteria, which will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option is not available.

NOTE: For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the **Event Log Trigger** or the **Joined Dynamic Group Trigger** (see above). For more information, see the Throttling chapter.

Click **Finish** when you have defined the recipients of this task and the triggers that execute the task.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

Agent deployment can be performed in a few different ways. You can deploy the Agent:

Remotely - using a Server task for mass deployment of the ERA Agent, alternatively you can deploy the Agent using GPO and SCCM
Locally - using an Agent installation package or Agent Live Installers, for example, if problems occur during remote deployment

Local deployment can be performed in three ways:

- Agent Live Installers - using a generated script from within the ERA Web Console, you can distribute Agent Live Installers via email or run them from removable media (USB flash drive, etc.)
- Server assisted installation - using the Agent installation package downloads certificates from the ERA Server automatically (recommended local deployment method)
- Offline installation - using the Agent installation package, you must manually export certificates and use them in this deployment method

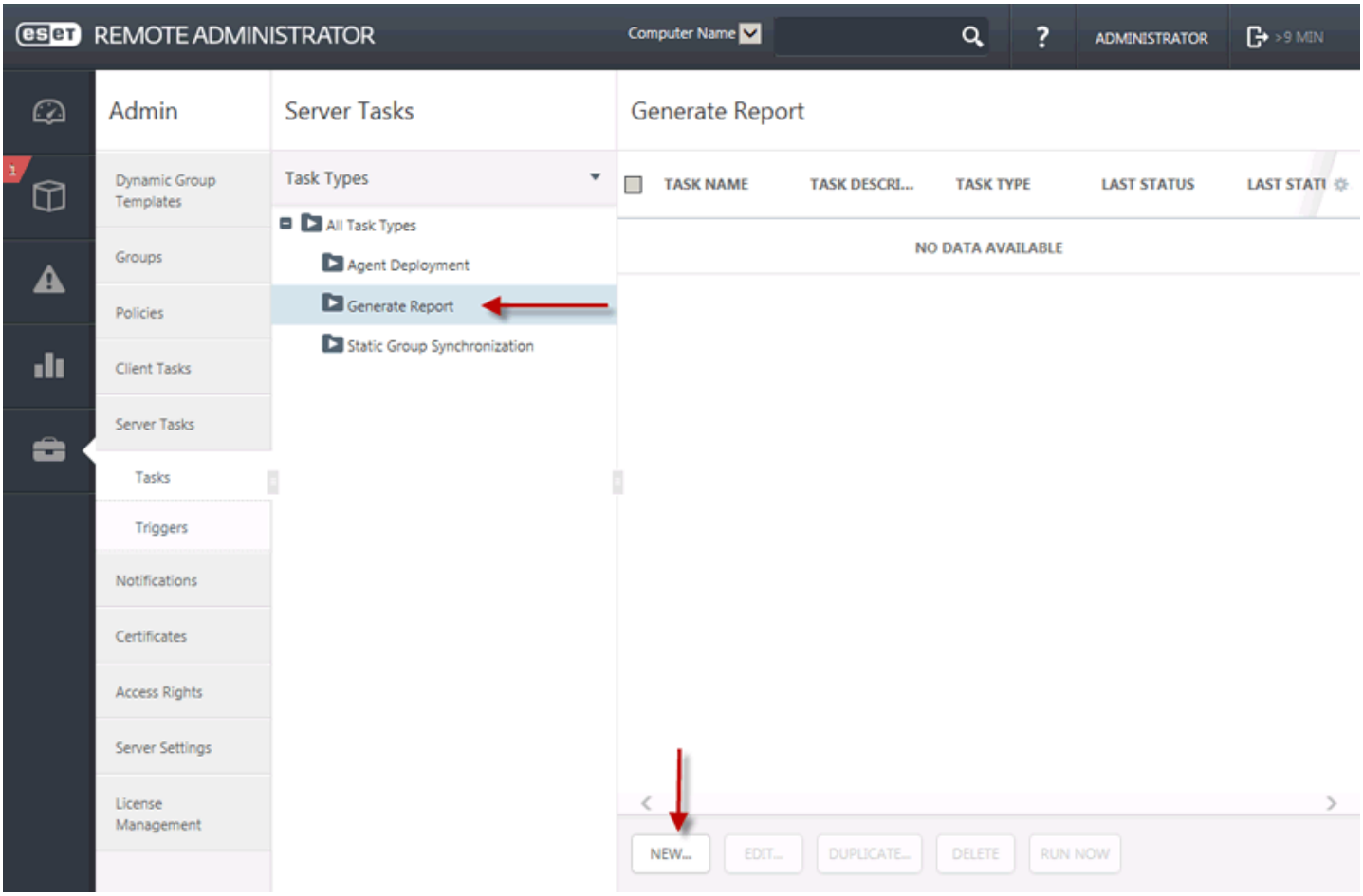
The Remote Agent deployment server task can be used for mass distribution of the Agent to client computers. It is the most convenient distribution method since it can be performed from Web Console without the need to deploy the Agent to each computer manually.

ERA Agent is very important because ESET security solutions running on client computers communicate with ERA Server exclusively through the Agent.

NOTE: Should you experience problems when deploying the ERA Agent remotely (the Server task **Agent deployment** fails) see the Troubleshooting guide.

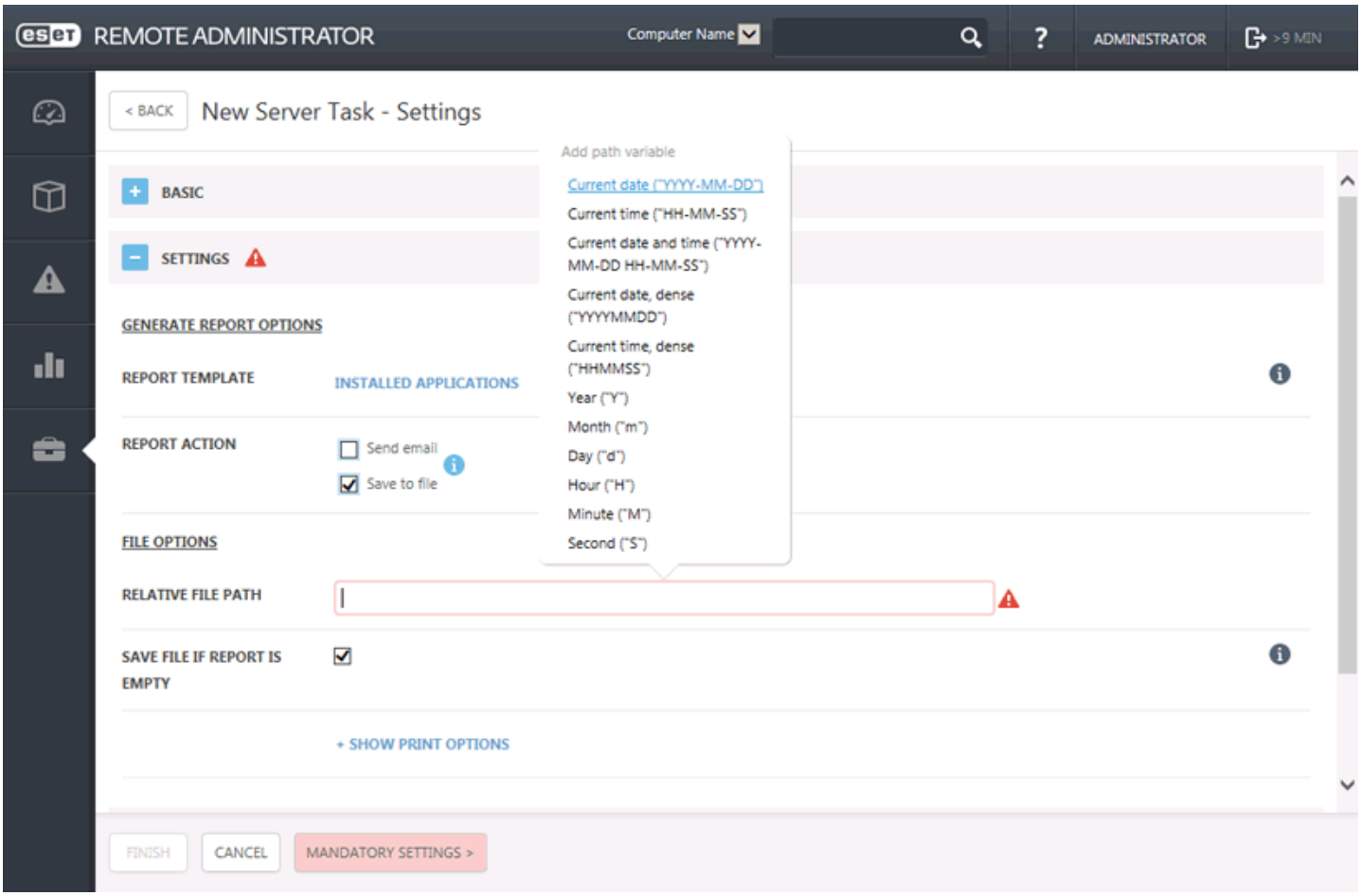
6.1.4.2.2 Generate Report

The **Generate Report** task is used to generate reports from previously created or pre-defined Report templates.



Settings

Report template - Choose a report template from the list.



Select Send email or Save to file to get the generated report.

SEND EMAIL

To send/receive mail messages, you must configure SMTP settings under Server Settings > **Advanced Settings**.

Mail message

- **Send to** - Enter the email address(-es) of recipients for report emails. Separate multiple addresses with a comma (,). It is also possible to add CC and BCC fields; these work exactly as they do for mail clients.
- **Subject** - Subject of the report message. Enter a distinctive subject, so that incoming messages can be sorted. This is an optional setting, but we recommend that you do not leave it empty.
- **Message contents** - Define the body of the report message.
- **Send mail if report is empty** - use this option if you want the report to be sent even though there is no data in it.

Print options

Click **Show print options** to display the following settings:

- **Output format** - Select the appropriate file format. The generated report will be attached to the message and can be printed later.
- **Output language** - Select the language for the message. The default language is based on the language selected for the ERA Web Console.
- **Page size/Resolution/Paper orientation/Color format/Margin units/Margins** - These options are relevant if you want to print the report. Select the appropriate options based on your print preferences. These options only apply to the PDF and PS format, not to the CSV format.

NOTE: The **Generate report** task allows you to select from several output file formats. Selecting CSV results in the date and time values in your report to be stored in the UTC format. When you select either of the two remaining output options (PDF, PS) the report will use the local server time.

SAVE TO FILE

File options

- **Relative file path** - The report will be generated in a specific directory, for example: *C:\Users\All Users\ESET\RemoteAdministrator\Server\Data\GeneratedReports*
- **Save file if report is empty** - use this option if you want the report to be saved even though there is no data in it.

Print options

Click **Show print options** to display the following settings:

- **Output format** - Select the appropriate file format. The generated report will be attached to the message and can be printed later.
- **Output language** - Select the language for the message. The default language is based on the language selected for the ERA Web Console.
- **Page size/Resolution/Paper orientation/Color format/Margin units/Margins** - These options are relevant if you want to print the report. Select the appropriate options based on your print preferences. These options only apply to the PDF and PS format, not to the CSV format.

NOTE: The **Generate report** task allows you to select from several output file formats. Selecting CSV results in the date and time values in your report to be stored in the UTC format. When you select either of the two remaining output options (PDF, PS) the report will use the local server time.

Triggers

Select an existing trigger for this task, or create a new trigger. It is also possible to **Remove** or **Modify** a selected trigger.

Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

NOTE: The Ubuntu Server Edition requires **X Server** and **xinit** installed for the correct function of the Report Printer (PDF Reports).

```
sudo apt-get install server-xorg
sudo apt-get install xinit
startx
```

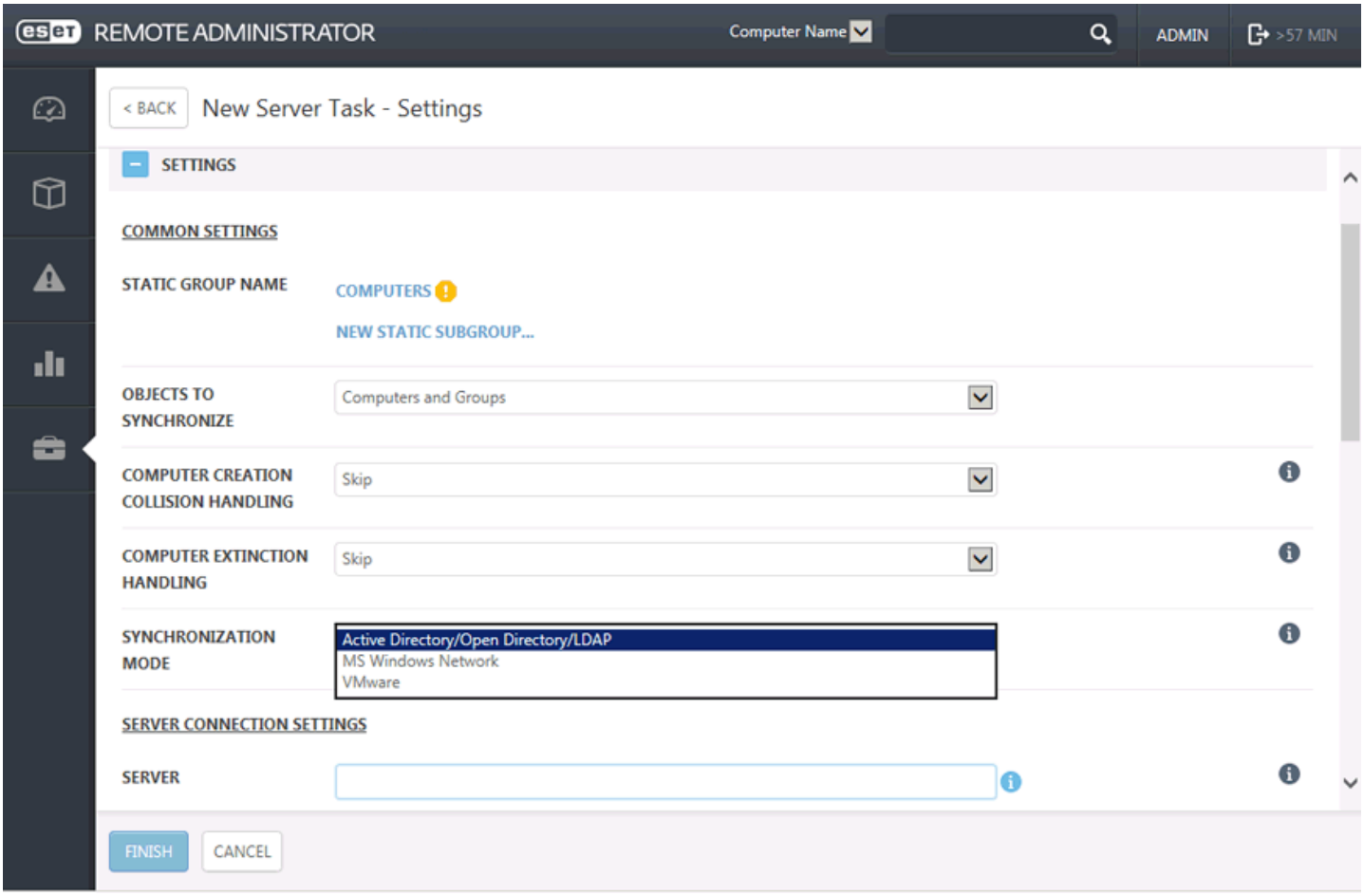
6.1.4.2.3 Static Group Synchronization

The **Static Group Synchronization** task will search your network (Active Directory, Mac open Directory, LDAP, local network) for computers and put them into a Static group. If you select **Synchronize with Active Directory** during Server Installation, computers that are found are added to the **All** group.

Click **Admin** > **Server Task** >**Static Group Synchronization** > **New...** to start configuring your new task.

Basic

Enter basic information about the task, such as the **Name**, **Description** (optional). The **Task Type** defines the settings and behavior of the task. Select the check box next to **Run task immediately after finish** to have the task run automatically after you click **Finish**.



Settings

- **Static group name** - This group will be the root for synchronized computers.
- **Object to synchronize** - Either **Computers and Groups**, or **Only Computers**.
- **Computer creation collision handling** - If the synchronization adds computers that are already members of the Static Group, you can select a conflict resolution method: **Skip** (synchronized computers will not be added), **Move** (new computers will be moved to a subgroup) or **Duplicate** (new computers will be added with a different name).
- **Computer extinction handling** - If a computer no longer exists, you can either **Remove** this computer or **Skip** it.

Synchronization mode:

- **Active Directory/Open Directory/LDAP -** Enter the basic **Server connection information** (Server name, Login, Password).
- **MS Windows Network -** Enter a **Workgroup** to be used and the user with his credentials (Login & Password).
- **VMware -** Enter hostname or IP address and credentials used to access VMware vCenter Server.

Server connection settings:

- **Server** - Type the Servername or IP address of your domain controller.
- **Login** - Type the login credentials for your domain controller in the format **domain\username**.
- **Password** - Type the password used to log onto your domain controller.

- **Use LDAP Parameters -** If you want to use LDAP, select check box **Use LDAP instead of Active Directory** and enter specific attributes to match your server, or you can select a **Preset** by clicking **Custom...** and the attributes will be populated automatically.

Synchronization settings:

- **Distinguished name** - Path (Distinguished Name) to the node in the Active Directory tree. Leaving this option empty will synchronize the entire AD tree.
- **Excluded distinguished name(s)** - You can choose to exclude (ignore) specific nodes in the Active Directory tree.
- **Ignore disabled computers (only in active directory)** - You can select to ignore computers disabled in active directory, the task will skip these computers.

Triggers

Select an existing trigger for this task, or you can create a new trigger. It is also possible to **Remove** or **Modify** a selected trigger.

Summary

Review the configuration information displayed here and if it is ok, click **Finish**. The task is now created and ready to be used.
Only Windows computers are recipients by default. If you have Linux computers in your Windows domain and want them to be the recipients of this task as well, make them visible first. Linux computers in a Windows domain don`t display any text in ADUC (Active Directory Users and computers) computer properties, so this information must be entered manually.

6.1.4.2.4 Static Group Synchronization - Linux Computers

Linux computer joined to Windows domain does not display any text in Active Directory Users and Computers (ADUC) in Computer properties, therefore it is necessary to insert text manually.

- Check the Server prerequisites and the following prerequisites:

- The Linux computers are in Active Directory.
- Domain controller has a DNS server installed.
- **ADSI Edit** is installed.

1. Open a command prompt and run adsiedit.msc
2. Navigate to **Action** > **Connect to**. The connection settings windows will be displayed.
3. Click **Select a well known Naming context**.
4. Expand the combo box below and select **Default** naming context.
5. Click **OK** - the ADSI value on the left should be the name of your domain controller - Default naming context (your domain controller).
6. Click the **ADSI** value and expand its subgroup.
7. Click the **subgroup** and navigate to the CN (Common Name) or OU (Organizational Unit) where Linux computers are displayed.
8. Click the **hostname** of the Linux computer and select **Properties** from the context menu. Navigate to the **dNSHostName** parameter and click **Edit**.
9. Change the value **<not set>** to valid text (for example, *ubuntu.TEST*).
10. Click **OK** > **OK**. Open **ADUC** and select the **properties** of the Linux computer - the new text should be displayed here.

6.1.4.3 Scheduling Server Task

Scheduled Trigger will run the task based on a date and time settings. Task can be scheduled to **run once**, on repetitive base or on CRON expression.

6.1.4.4 Reuse Trigger in Server Task

Reuse of a server trigger means that the same trigger (circumstance/event) is able to initiate multiple tasks (actions) at the same time.

For example, consider a situation where the ERA user needs to generate 2 different periodic monthly reports at the same time. Follow the steps below to reuse the trigger for the first report to create the second.

1. Create the first Generate report task with an assigned Monthly scheduled trigger.
2. Start to configure the second Generate report task with a different report.
3. In the **Triggers** screen of the task creation wizard click **Add** existing. The list of existing triggers will be displayed.
4. Pick the same Monthly scheduled trigger which was used for the first **Generate report** task.
5. **Save** the task. After these steps 2 different reports will be generated each month at the same time.

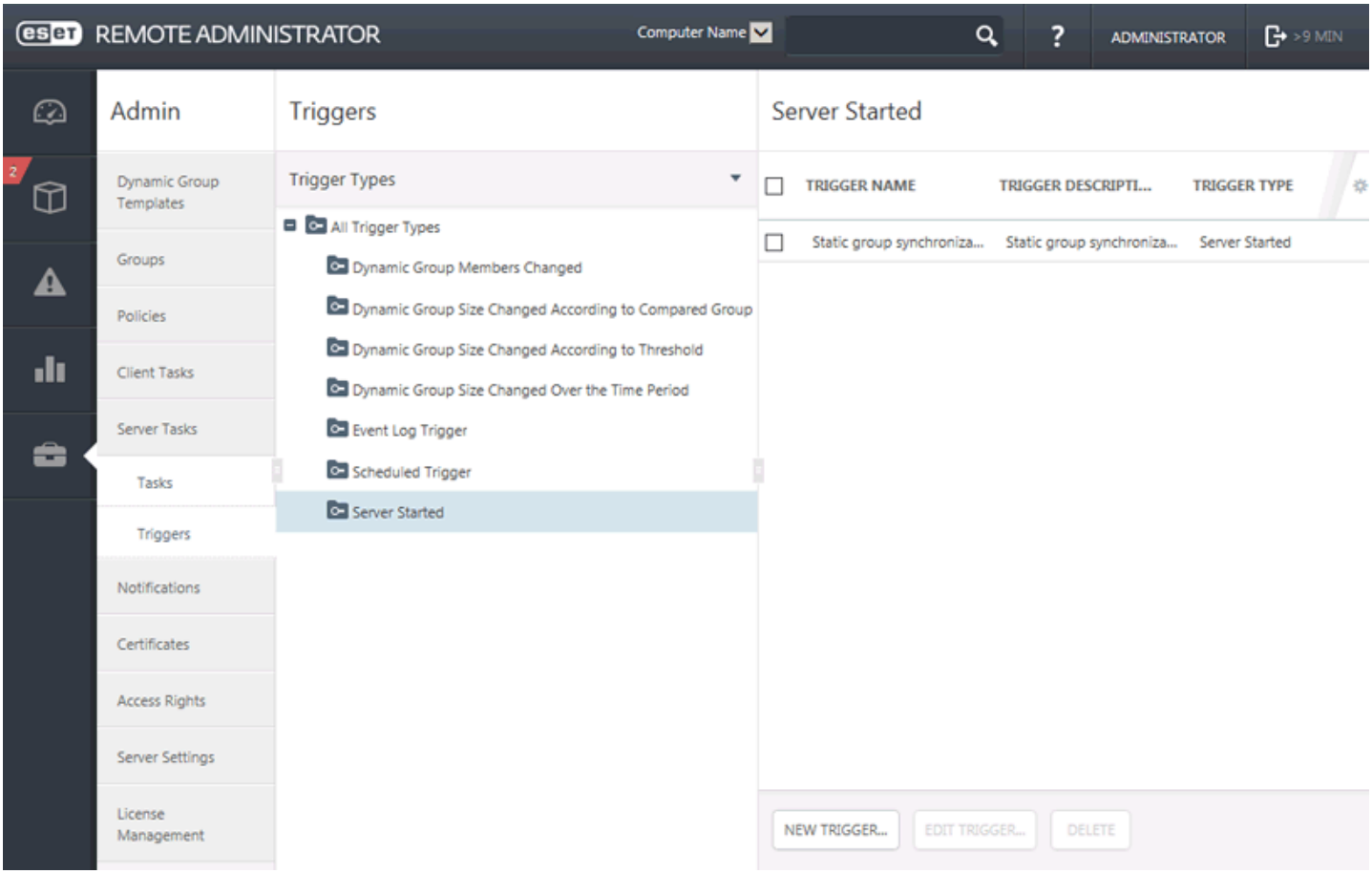
6.1.4.5 Triggers

Triggers are basically sensors that react to certain events in a pre-defined way. They are used to execute an action (in most cases, to run a task). They can be activated by the scheduler (time events) or when a certain system event occurs.

A trigger executes all tasks assigned to the trigger at the moment when the trigger is activated. The trigger does not run newly assigned tasks immediately—they are ran as soon as the trigger is fired. Trigger sensitivity to events can be reduced further using throttling.

Server Trigger Types:

- **Dynamic Group Members Changed -** This trigger is invoked when the contents of a Dynamic Group change. For example, if clients join or leave a Dynamic Group called *Infected*.
- **Dynamic Group Size Changed According to Compared Group -** This trigger is invoked when the number of clients in an observed Dynamic Group change according to a compared group (static or dynamic). For example, if more than 10% of all computers are infected (the group **All** compared to the group **Infected**).
- **Dynamic Group Size Changed According to Threshold -** This trigger is invoked when the number of clients in a Dynamic Group becomes higher or lower than the specified threshold. For example, if more than 100 computers are in the group **Infected**.
- **Dynamic Group Size Changed Over the Time Period -** This trigger is invoked when the number of clients in a Dynamic Group changes over a defined time period. For example, if the number of computers in the group Infected increases by 10% in an hour.
- **Event Log Trigger -** This trigger is invoked when a certain event occurs in logs. For example, if there is a threat in the Scan log.
- **Scheduled Trigger -**This trigger is invoked at a certain time and date.
- **Server Started -** Is invoked when the server starts. For example, this trigger is used for the Static Group Synchronization task.



6.1.4.5.1 Throttling

Under defined circumstances, throttling may prevent a trigger from firing. Time-based conditions take precedence over statistical conditions.

If any of the conditions are met, all state information of all observers is reset (observation starts from scratch). This holds for Time-Based as well as Statistical conditions. State information for observers is not persistant, they are reset even if the Agent or Server is restarted.

Any modification made to a trigger causes a reset of its status.

There are several ways to control triggering:

Statistical

Statistical triggers fire based on any combination of the following parameters:

- S1: Trigger should fire every **N** occurrences of the triggering event (modulo **N**) starting with last event in a series (for example, from start, wait for the Nth event)
- S2: Trigger if **N** events occur within **X time** (the time can be chosen from a pre-defined set) [**N** <= 100] in floating total sense – only the count of events during the last X time is taken into account. Firing of the trigger causes a buffer reset
- S3: **N** events with unique symbol **S** occur [N <= 100] in a row. The buffer is reset if the trigger is fired and there is an event already in buffer. The Buffer is in the mode “floating window” – FIFO queue. The new symbol is compared with every symbol in the buffer.
  Note: A missing value (n/a) is considered as not unique and therefore the buffer is reset since last triggered

These conditions can be combined with the AND operator (all of the set ones must be satisfied) or the OR operator (whichever occurs first).

Time based

All of the following conditions must be satisfied simultaneously (if set):

- T1: The trigger may run within **X time range**. Range is given as a repeated series of marginal times (for example, between 13:00 – 14:00 OR 17:00 – 23:30)
- T2: The trigger can be executed at most once every **X time**.

Additional Properties

As stated above, not every event will cause a trigger to fire. Actions taken for non-firing events can be:

- If there is more than one event skipped, group the last **N** events into one (store data of suppressed ticks) [**N** <= 100]
- for **N** == 0, only the last event is processed (**N** means history length, the last event is always processed)
- All non-firing events are merged (merging the last tick with **N** historical ticks)

Examples:

S1: Criterion for occurrences (allow every 3rd tick)

Time	00	01	02	03	04	05	06	trigger is modified	07	08	09	10	11	12	13	14	15
Ticks	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: Criterion for occurrences within time (allow if 3 ticks occur within 4 seconds)

Time	00	01	02	03	04	05	06	trigger is modified	07	08	09	10	11	12	13

Ticks	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Criterion for unique symbol values (allow if 3 unique values are in a row)

Time	00	01	02	03	04	05	06	trigger is modified	07	08	09	10	11	12	13
Value	A	B	B	C	D	G	H		J	K	n/a	L	M	N	N
S3					1									1	

S3: Criterion for unique symbol values (allow if 3 unique values are since the last tick)

Time	00	01	02	03	04	05	06	07	trigger is modified	08	09	10	11	12	13	14
Value	A	B	B	C	D	G	H	I		J	K	n/a	L	M	N	N
S3				1			1						1			

T1: Allow a tick in certain time ranges (allow every day starting at 8:10, duration 60 seconds)

Time	8:09:50	8:09:59	8:10:00	8:10:01	trigger is modified	8:10:59	8:11:00	8:11:01
Ticks	x	x	x	x		x	x	x
T1			1	1		1		

This criterion has no state; therefore trigger modifications have no effect on the results.

T2: Allow a single tick in a time interval (allow at most once every 5 seconds)

Time	00	01	02	03	04	05	06	trigger is modified	07	08	09	10	11	12	13
Ticks	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

S1+S2 combination

- S1: every 5th tick
- S2: 3 ticks within 4 seconds

Time	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Ticks	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Result			1				1								1		

The result is enumerated as: S1 (logical or) S2

S1+T1 combination

- S1: Allow every 3rd tick
- T1: Allow every day starting at 8:08, duration 60 seconds

Time:	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Ticks	x	x	x	x	x	x	x	x	x	x

S1			1			1			1	
T1					1	1	1	1	1	
Result						1			1	

The result is enumerated as: S1 (logical and) T1

S2+T1 combination

- S2: 3 ticks within 10 seconds
- T1: Allow every day starting at 8:08, for a duration of 60 seconds

Time:	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Ticks	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Result							1			

The result is enumerated as: S2 (logical and) T1.
Note that the state of S2 is reset only when the global result is 1.

S2+T2 combination

- S2: 3 ticks within 10 seconds
- T2: Allow at most once every 20 seconds

Time:	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Ticks	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Result			1													1		

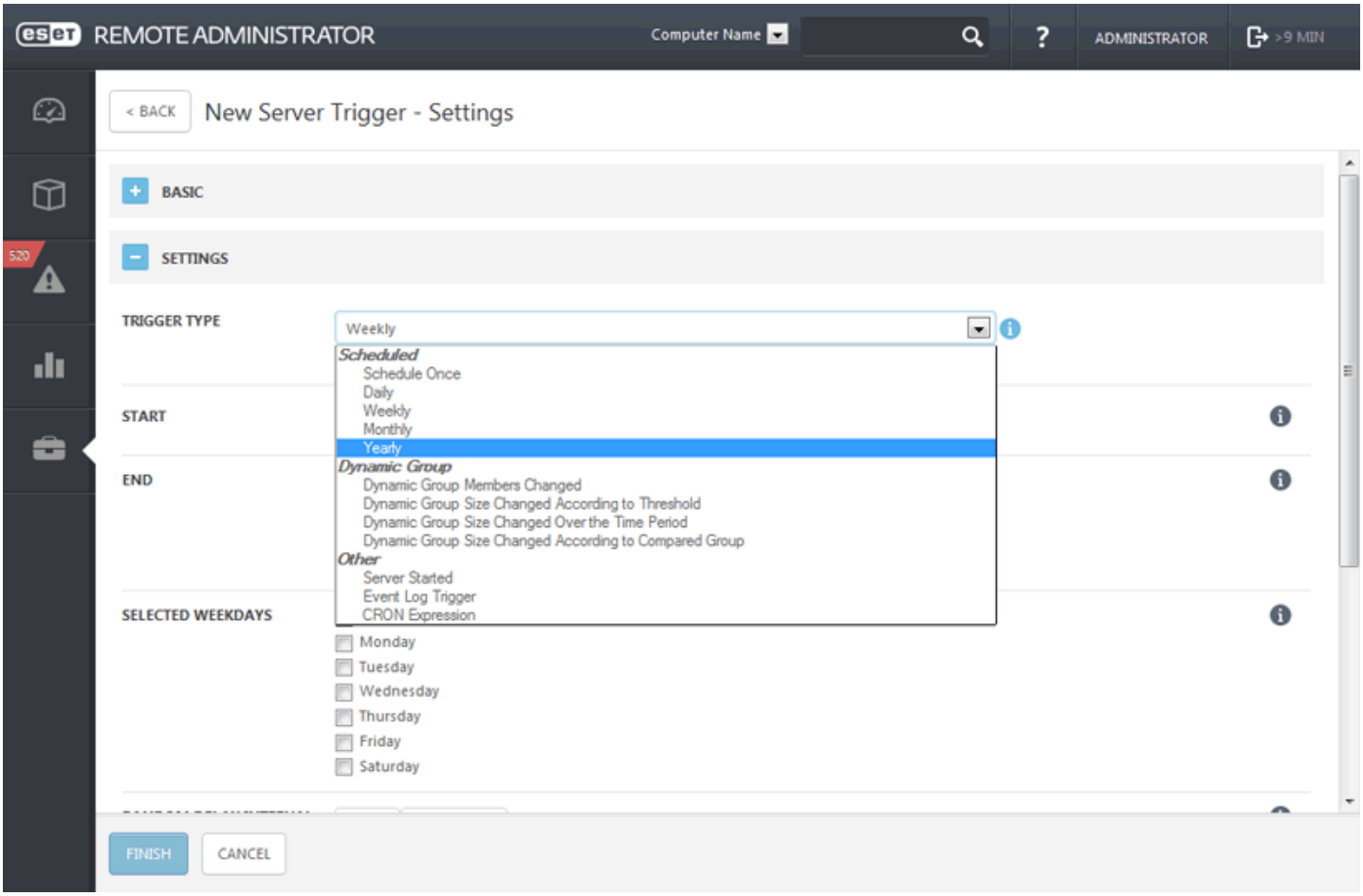
The result is enumerated as: S2 (logical and) T2.
Note that the state of S2 is reset only when the global result is 1.

6.1.4.5.1.1 Trigger is too sensitive

Use the same throttling conditions shown in the Trigger fires too often section of this guide.

6.1.4.5.2 Server Trigger Wizard

Triggers are created and managed in the **Admin** tab > **Server tasks** > **Triggers.** Select **Triggers type** > **New Trigger.**



6.1.4.5.3 Manage Server Triggers

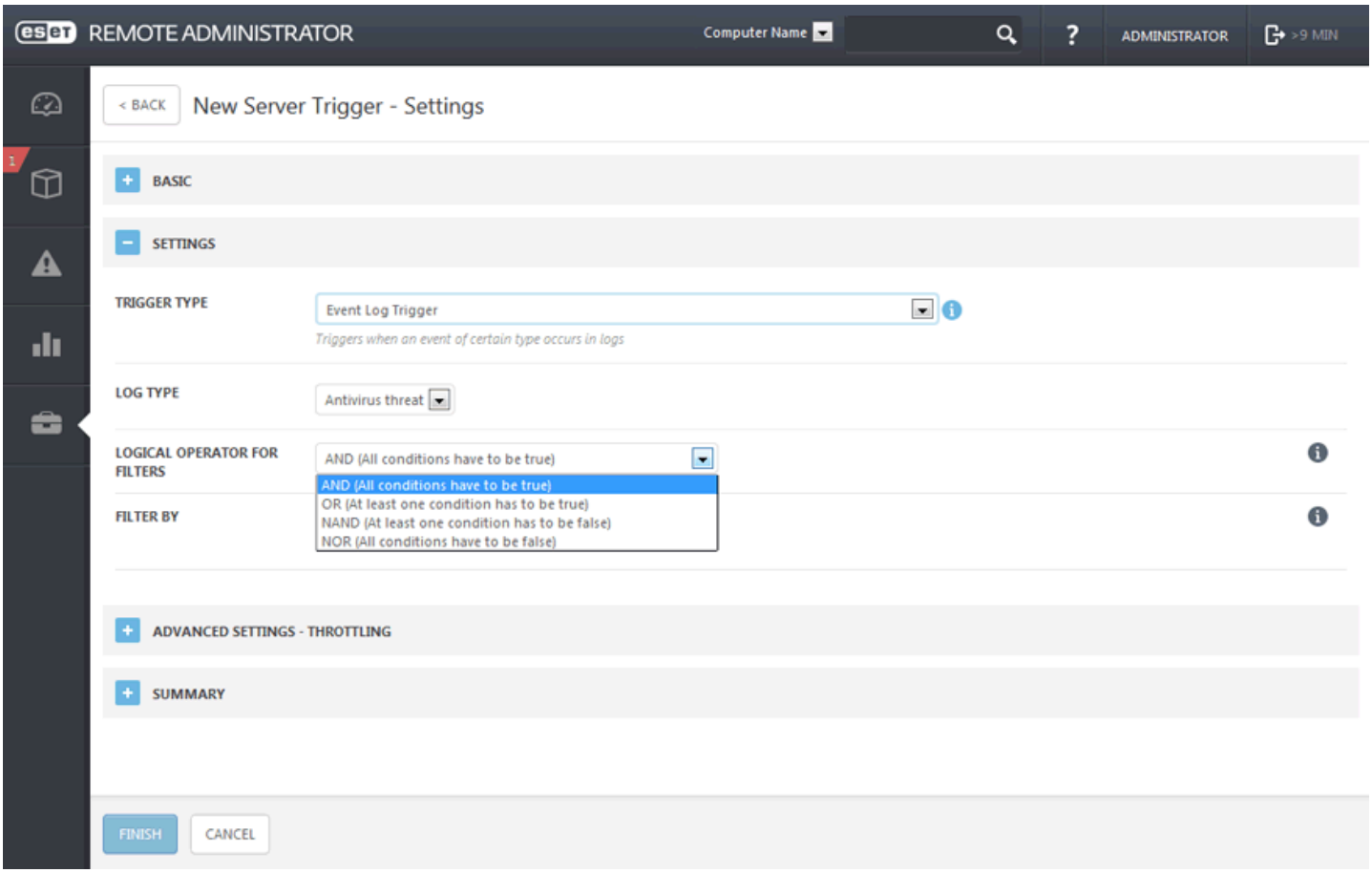
To manage Server Triggers, from the **Admin** tab click **Server tasks** > **Triggers**, select **Trigger type** and click **Edit.**

Basic

Define a **name** for your trigger, you can also enter a **description** of the trigger if you want.

Settings

- Select a trigger type. Trigger type defines the method to activate the trigger. Select an **Event Log Trigger** and continue.
- Select a **log type**. The trigger is activated when a certain event occurs in this log.
- Define the event that has to occur in order to activate the trigger. Select a **logical operator** for filtering the events. In this example, select **AND (All conditions have to be true)**.
- If you need add a **filter** from the list (as event) and select the logical operator for the custom string.

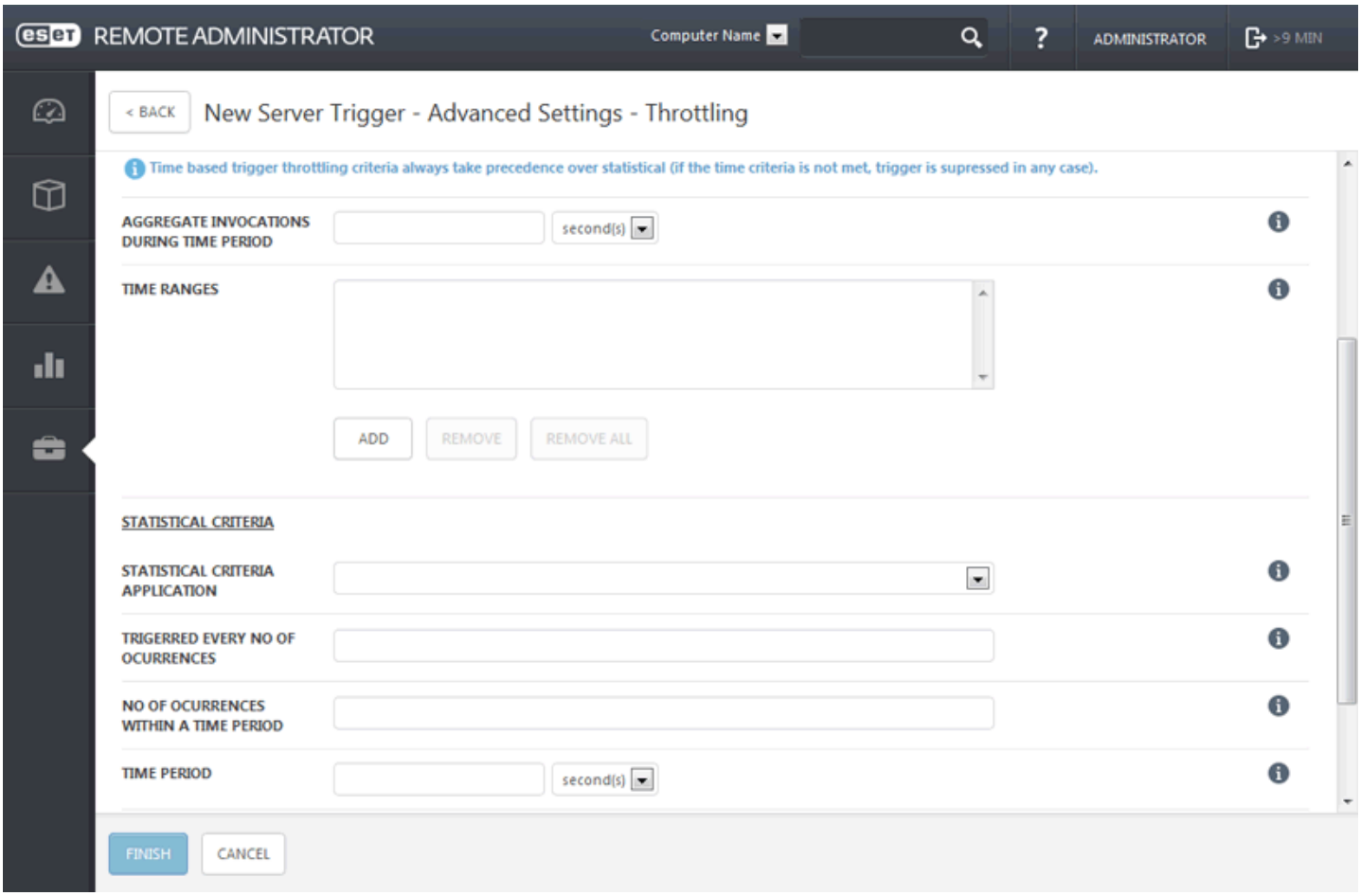


Select a logical operator in the **Operation** menu.

- **AND** - All defined conditions have to be true.
- **OR** - At least one condition has to be true.
- **NAND** - At least one condition has to be false.
- **NOR** - All conditions have to be false.

Advanced Settings - Throttling

Specify the **Number of ticks to aggregate**. This will define how many ticks (trigger hits) are needed in order to activate the trigger. For more specific information, see the Throttling chapter.



Summary

Review the settings of your new trigger, make adjustments and click **Finish**. Your trigger is now saved on the server and ready to be used. You can also view triggers that you have created in the list on the right. To edit or delete the trigger, simply click the trigger in the list and select the appropriate action from the context menu. To delete multiple triggers at once, select the check boxes next to the triggers you want to remove and click **Delete**.

6.1.4.5.3.1 Trigger fires too often

If you want to be notified less often, consider the following suggestions:

- If the user wants to react only if there are more events, not a single one, see statistical condition S1 in Throttling.
- If the trigger should fire only when a cluster of events occur, follow statistical condition S2 in Throttling.
- When events with unwanted values are supposed to be ignored, refer to statistical condition S3 in Throttling.
- When events from outside relevant hours (for example, working hours) should be ignored, see time-based condition T1 in Throttling.
- To set a minimum time between trigger firings, use time-based condition T2 in Throttling.

NOTE: The conditions can also be combined to form more complex throttling scenarios.

6.1.4.5.3.2 CRON Expression

A CRON Expression is used to configure specific instances of a trigger. It is a string consisting of 7 subexpressions (field), that represent individual values of the schedule. These fields are separated by a space, and they can contain any of the allowed values with various combinations.

Name	Required	Value	Allowed Special Characters
Seconds	Yes	0-59	,-*/
Minutes	Yes	0-59	,-*/
Hours	Yes	0-23	,-*/
Day of the month	Yes	1-31	,-*/ L W C
Month	Yes	0-11 or JAN-DEC	,-*/
Day of the week	Yes	1-7 or SUN-SAT	,-*/ L C #
Year	No	empty or 1970-2099	,-*/

Examples are available here.

6.1.4.5.4 Manage Trigger Sensitivity

Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event. Under certain circumstances, throttling may prevent a trigger from being fired. If any of the defined conditions are met, stacked information for all observers is reset (the count starts over from 0). This information is also reset if the Agent or ERA Server are restarted. All modifications made to a trigger reset its status.

Time-based throttling conditions take precedence over statistical conditions. We recommend that you only use one statistical condition and multiple time-based conditions. Multiple statistical conditions can be an unnecessary complication, and can alter trigger results.

- **Statistical conditions**

The Statistical conditions can be combined either using the **AND** logical operator (all conditions must be fulfilled) or with the **OR** logical operator (the first condition fulfilled triggers the action).

- **Time based conditions**

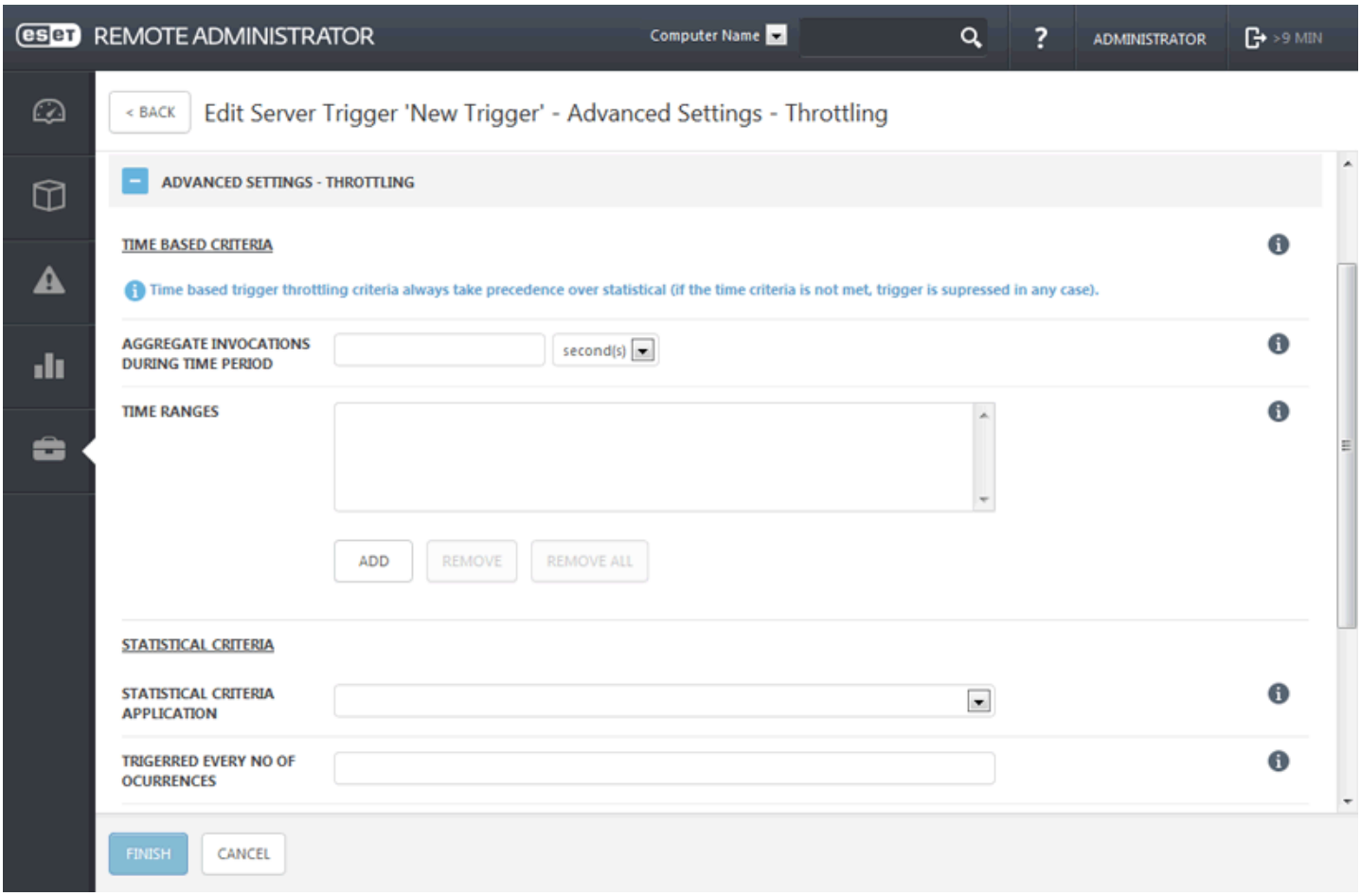
All of the configured conditions must be fulfilled in order to trigger an event. The throttling criteria are focused on the time when the event occurred.

Aggregation

- **Number of ticks to aggregate** - Number of ticks (how many times the trigger is hit) needed to activate the trigger. The trigger is prevented from activating until this number is reached. For example, with this set to 100, if 100 threats are detected you won't receive 100 notifications, just one notification containing 100 threats. If 200 threats are detected, only the last 100 threats will be included in the notification.

Time based criteria

- **Aggregate invocations during time period** - You can allow a hit once every X seconds. If you set this option to 10 seconds and during this time 10 invocations occur, only 1 will be counted.
- **Time ranges** - Allow ticks only within the defined time period. You can add multiple time ranges to the list, they will be sorted chronologically.



Statistical criteria

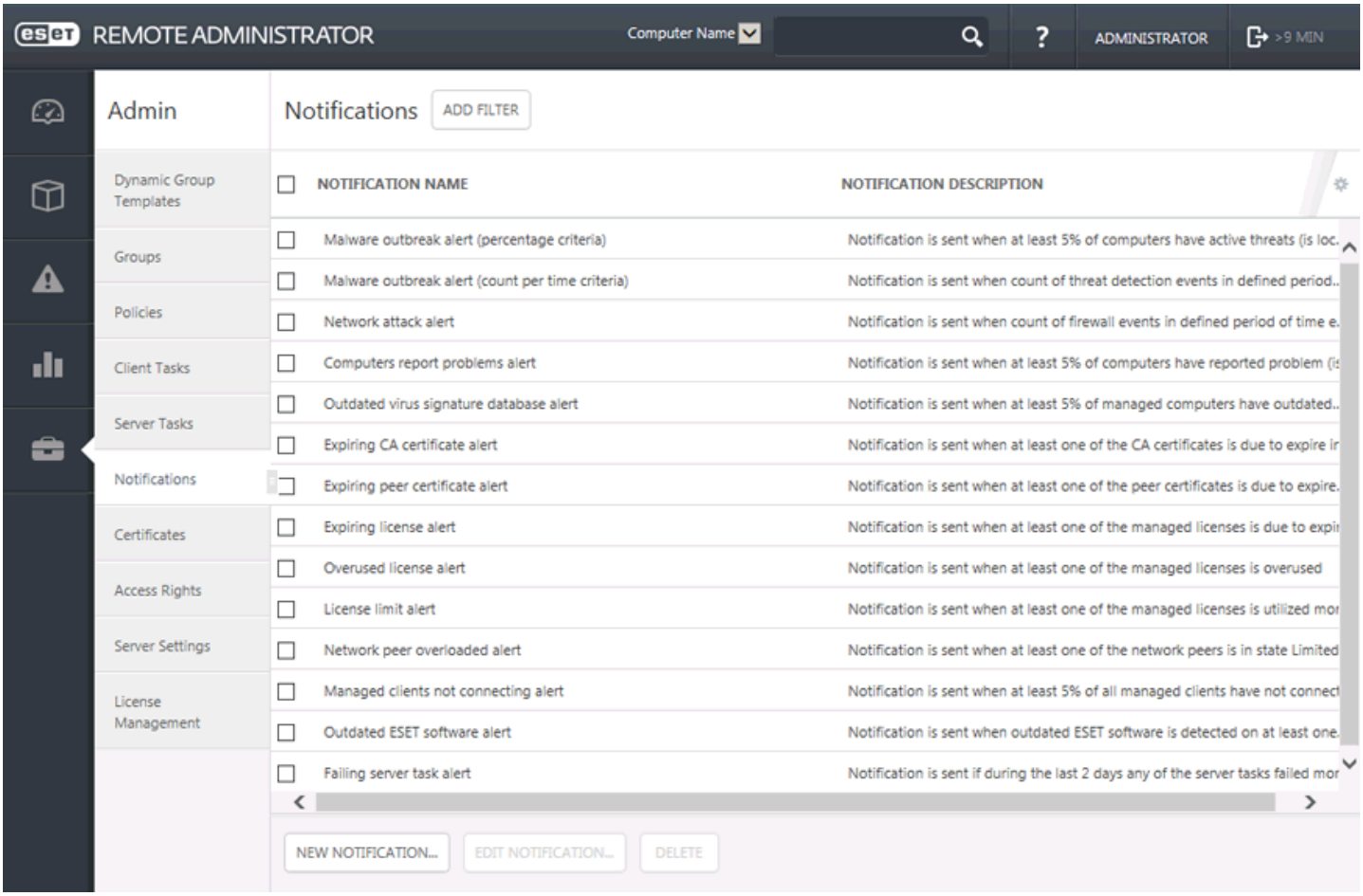
- **Statistical criteria application** - This option defines the method by which the statistical criteria will be evaluated. Either all of them need to be met (**AND**), or at least one (**OR**).
- **Triggered every No of occurrences** - Allow only every **X** tick (hit). For example, if you enter 10, only each 10th tick will be counted.
- **No of occurrences within a time period** - Allow only tick(s) within the defined time period. This will define the frequency. For example, allow the execution of the task if the event is detected 10x in an hour.
  - **Time period** - Define the time period for the option described above.
- **Number of events with symbol** - Record a tick(hit) if **X** events with the specific symbol are provided. For example, if you enter 10, a tick will be counted for every 10th installation of a certain application.
  - **Applies when number of events** - Enter a number of events in a row after the last tick to count another tick. For example, enter 10 and a tick will be counted after 10 events from the last tick.

- **Applies when number of events** - The trigger is applied when the ticks are either **Received in a Row** (trigger execution is not taken into account), or **Received Since Last Trigger Execution** (when the trigger is executed, the number is reset to 0).

6.1.5 Notifications

Notifications are essential for keeping track of the overall state of your network. When a new event occurs (based on your configuration), you will be notified using a defined method (either an SNMP Trap or email message), and you can respond accordingly.

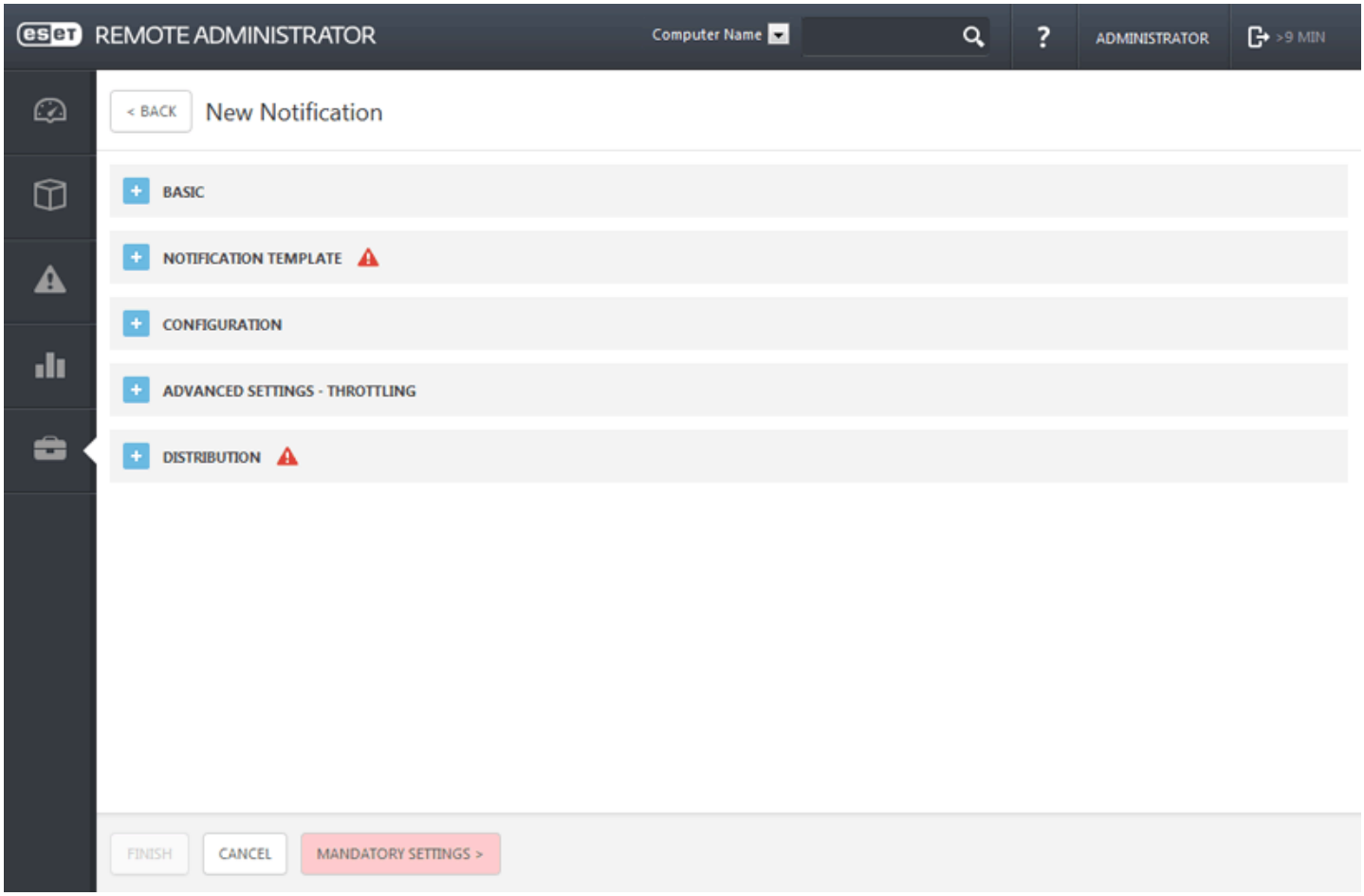
- All notification templates are displayed in the list, and it is possible to filter them based on the **Name** or the **Description**.
- Click **Add Filter** to add filtering criteria and/or enter a string into the **Name**/**Notification** field.
- Selecting an existing notification gives you the option to **Edit** it or **Delete** it completely.
- To create a new notification, click New notification on the bottom of the page.


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
>9 MIN
Admin
Notifications
ADD FILTER
Dynamic Group Templates
Groups
Policies
Client Tasks
Server Tasks
Notifications
Certificates
Access Rights
Server Settings
License Management
NOTIFICATION NAME
NOTIFICATION DESCRIPTION
Malware outbreak alert (percentage criteria)
Notification is sent when at least 5% of computers have active threats (is loc
Malware outbreak alert (count per time criteria)
Notification is sent when count of threat detection events in defined period
Network attack alert
Notification is sent when count of firewall events in defined period of time e
Computers report problems alert
Notification is sent when at least 5% of computers have reported problem (i
Outdated virus signature database alert
Notification is sent when at least 5% of managed computers have outdated
Expiring CA certificate alert
Notification is sent when at least one of the CA certificates is due to expire ir
Expiring peer certificate alert
Notification is sent when at least one of the peer certificates is due to expire
Expiring license alert
Notification is sent when at least one of the managed licenses is due to expi
Overused license alert
Notification is sent when at least one of the managed licenses is overused
License limit alert
Notification is sent when at least one of the managed licenses is utilized mo
Network peer overloaded alert
Notification is sent when at least one of the network peers is in state Limited
Managed clients not connecting alert
Notification is sent when at least 5% of all managed clients have not connect
Outdated ESET software alert
Notification is sent when outdated ESET software is detected on at least one
Failing server task alert
Notification is sent if during the last 2 days any of the server tasks failed mor
NEW NOTIFICATION...
EDIT NOTIFICATION...
DELETE

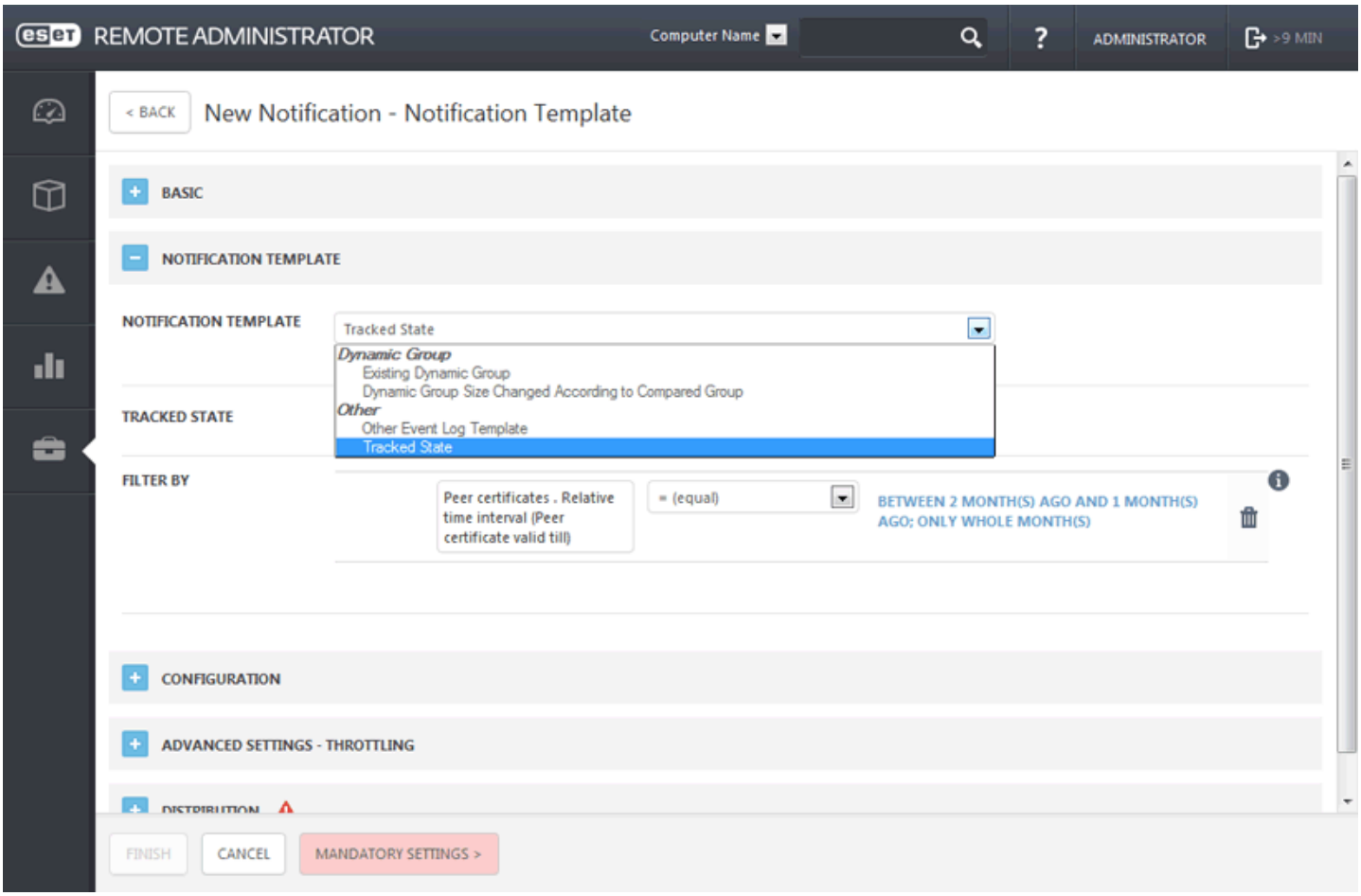
6.1.5.1 Notifications Wizard

Basic

Contains the **Name** and **Description** of the notification. This is important for filtering multiple notifications, the filter is located at the top of the **Notification** page.



Notification template



Existing Dynamic Group - An existing Dynamic Group will be used to generate notifications. Select a Dynamic Group from the list and click **OK**.
Dynamic Group Size Changed According to Compared Group - If the number of clients in an observed Dynamic Group changes according to a compared group (either static or dynamic), the notification will be invoked.**Other Event Log Template -** This option is used for notifications not associated with a Dynamic Group, but based on system events filtered out from the event log. Select a **Log type** on which the notification will be based and a **Logical operator** for filters.

Tracked State - This option notifies you on object state changes using the user defined filters.

Configuration

Notify every time the Dynamic Group content changes - Enable this to be notified of any changes when members in a Dynamic Group are added, removed or changed.
Notification time period - Define the time period (in minutes, hours or days) for the comparison with the new state. For example, 7 days ago, the number of clients with outdated security products was 10 and the **Threshold** (see below) was set to 20. If the number of clients with an outdated security product reaches 30, you will be notified.

Threshold - Define a threshold that will trigger the sending of a notification. You can either define a number of clients, or a percentage of clients (members of a Dynamic Group).
Generated message - This is a pre-defined message that will appear in the notification. It contains configured settings in a text form.
Message - Beside the pre-defined message, you can add a custom message (it will appear at the end of the pre-defined message above). This is optional, but it is recommended for better filtering of notifications.

NOTE: Configuration options may differ specific to different notification templates.

Advanced settings - Throttling

Time Based Criteria

- Specify the **Number of ticks to aggregate**. This will define how many ticks (trigger hits) are needed in order to activate the trigger. For more specific information, see the Throttling chapter.

Statistical criteria

- **Statistical criteria application** - This option defines the method by which the statistical criteria will be evaluated. Either all of them need to be met (**AND**), or at least one (**OR**).
- **Triggered every No of occurrences** - Allow only every **X** tick (hit). For example, if you enter 10, only each 10th tick will be counted.
- **No of occurrences within a time period** - Allow only tick(s) within the defined time period. This will define the frequency. For example, allow the execution of the task if the event is detected 10x in an hour. **Time period** - Define the time period for the option described above.
- **Number of events with symbol** - Allow a tick(hit) if **X** events with the specific symbol are provided. For example, if you enter 10, a tick will be counted for every 10 installation of a certain software. **Applies when number of events** - Enter a number of events in a row after the last tick to count another tick. For example, enter 10 and a tick will be counted after 10 events from the last tick.
- **Applies when number of events** - The trigger is applied when the ticks are either **Received in a Row** (trigger execution is not taken into account), or **Received Since Last Trigger Execution** (when the trigger is executed, the number is reset to 0).

Distribution

Subject - Subject of the message that contains the notification. This is optional, but also recommended for better filtering or when creating rules to sort notification messages.

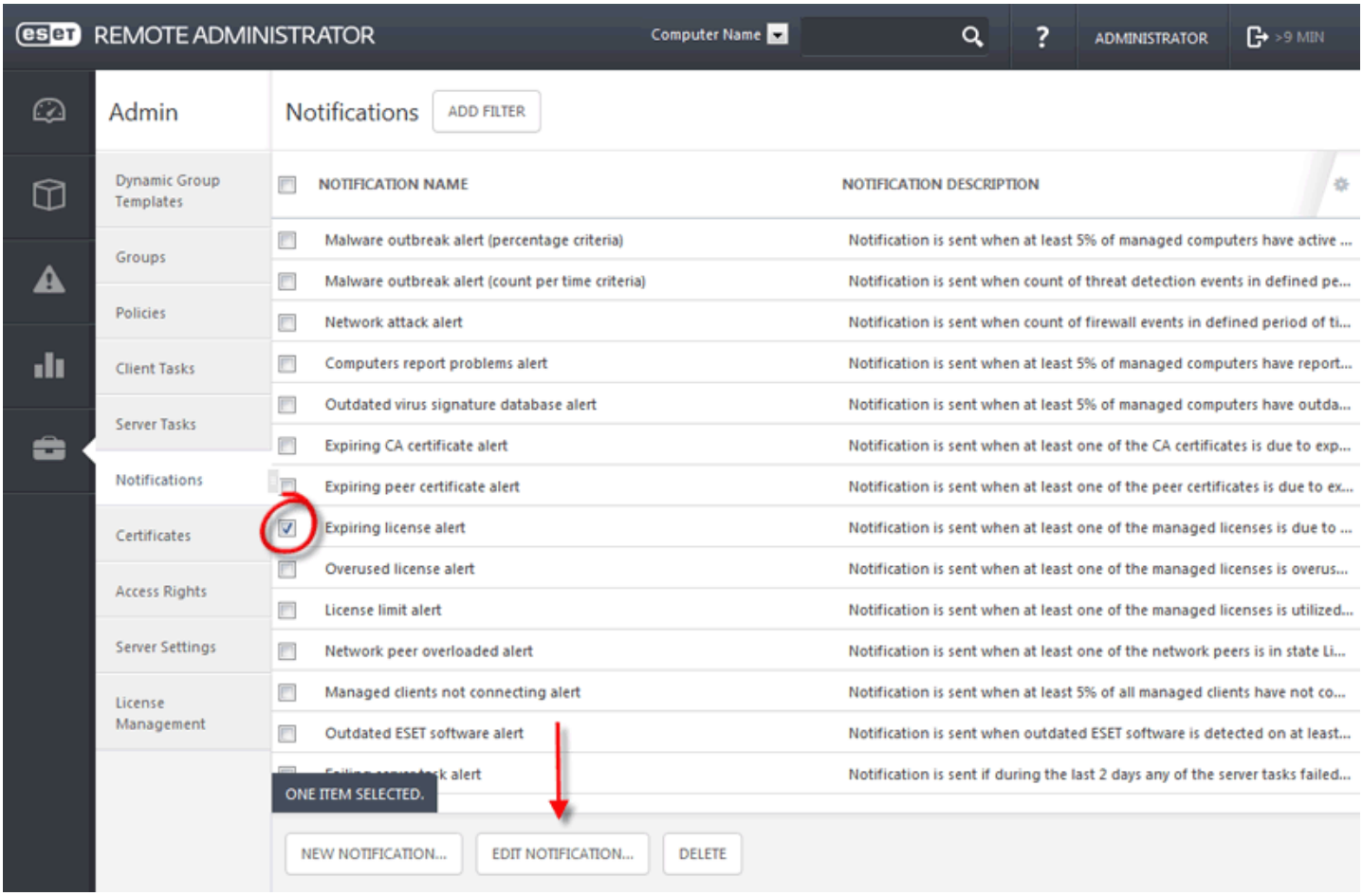
Distribution

- **Send SNMP Trap** - Sends an SNMP Trap. The SNMP Trap notifies the Server using an unsolicited SNMP message. For more information, see How to configure an SNMP Trap Service.
- **Send email** - Sends an email message based on your email settings.

Email addresses - Enter the email addresses of the recipients of the notification messages, separate multiple addresses with a comma (",").

6.1.5.2 Manage Notifications

Notifications are managed in the **Admin** tab. Select a notification and click **Edit Notification.**


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
>9 MIN
Admin
Notifications
ADD FILTER
Dynamic Group Templates
Groups
Policies
Client Tasks
Server Tasks
Notifications
Certificates
Access Rights
Server Settings
License Management
NOTIFICATION NAME
NOTIFICATION DESCRIPTION
Malware outbreak alert (percentage criteria)
Notification is sent when at least 5% of managed computers have active ...
Malware outbreak alert (count per time criteria)
Notification is sent when count of threat detection events in defined pe...
Network attack alert
Notification is sent when count of firewall events in defined period of ti...
Computers report problems alert
Notification is sent when at least 5% of managed computers have report...
Outdated virus signature database alert
Notification is sent when at least 5% of managed computers have outda...
Expiring CA certificate alert
Notification is sent when at least one of the CA certificates is due to exp...
Expiring peer certificate alert
Notification is sent when at least one of the peer certificates is due to ex...
Expiring license alert
Notification is sent when at least one of the managed licenses is due to ...
Overused license alert
Notification is sent when at least one of the managed licenses is overus...
License limit alert
Notification is sent when at least one of the managed licenses is utilized...
Network peer overloaded alert
Notification is sent when at least one of the network peers is in state Li...
Managed clients not connecting alert
Notification is sent when at least 5% of all managed clients have not co...
Outdated ESET software alert
Notification is sent when outdated ESET software is detected on at least...
Notification is sent if during the last 2 days any of the server tasks failed...
ONE ITEM SELECTED.
NEW NOTIFICATION...
EDIT NOTIFICATION...
DELETE

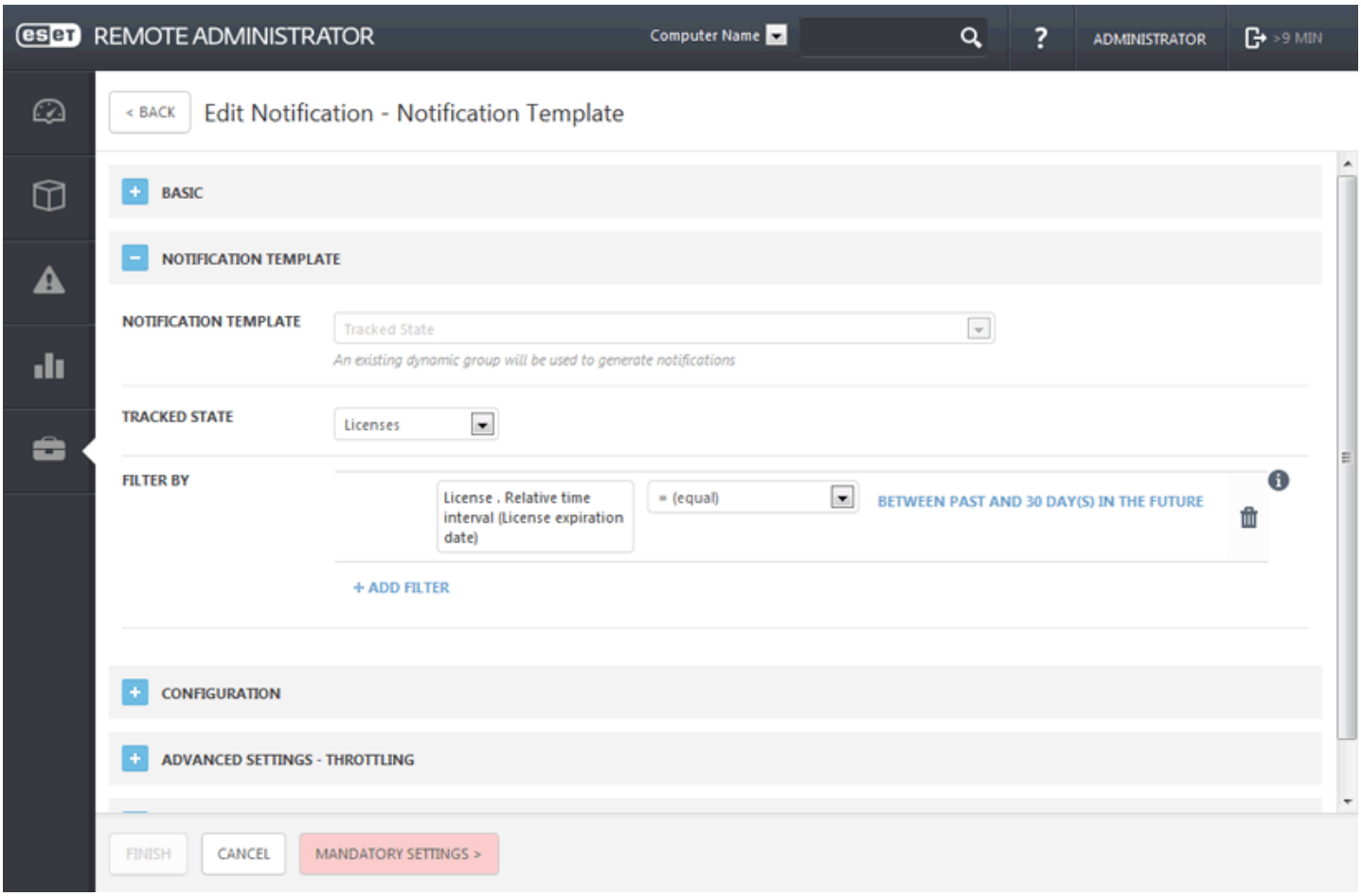
Basic

You can change **Notification Name** and **Description**. This is important for filtering multiple notifications.

Notification template

Existing Dynamic Group - An existing Dynamic Group will be used to generate notifications. Select a Dynamic Group from the list and click **OK**.
Dynamic Group Size Changed According to Compared Group - If the number of clients in an observed Dynamic Group changes according to a compared group (either static or dynamic), the notification will be invoked.
Other Event Log Template
This option is used for notifications not associated with a Dynamic Group, but based on system events filtered out from the event log. Select a **Log type** on which the notification will be based and a **Logical operator** for filters.
Tracked State - This option notifies on object state changes using the user defines filters.

NOTE: You can change Tracked state and **+ Add Filter** or **Logical operator** for filters.



Configuration

Notify every time the Dynamic Group content changes - Enable this to be notified of any changes when members in a Dynamic Group are added, removed or changed.
Notification time period - Define the time period (in minutes, hours or days) for the comparison with the new state. For example, 7 days ago the number of clients with outdated security products was 10 and the **Threshold** (see below) was set to 20. If the number of clients with an outdated security product reaches 30, you will be notified.
Threshold - Define a threshold that will trigger the sending of a notification. You can either define a number of clients, or a percentage of clients (members of the Dynamic Group).
Generated message - This is a pre-defined message that will appear in the notification. It contains configured settings in a text form.
Message - Beside the pre-defined message, you can add a custom message (it will appear at the end of the pre-defined message above). This is optional, but it is recommended for better filtering of notifications and overview.

NOTE: Available options depend on the selected notification template.

Advanced settings - Throttling

Time-Based Criteria

- Specify the **Number of ticks to aggregate**. This will define how many ticks (trigger hits) are needed in order to activate the trigger. For more specific information, see the Throttling chapter.

Statistical criteria

- **Statistical criteria application** - This option defines the method by which the statistical criteria will be evaluated. Either all of them need to be met (**AND**), or at least one (**OR**).
- **Triggered every No of occurrences** - Allow only every **X** tick (hit). For example, if you enter 10, only each 10th tick will be counted.
- **No of occurrences within a time period** - Allow only tick(s) within the defined time period. This will define the frequency. For example, allow the execution of the task if the event is detected 10x in an hour. **Time period** - Define the time period for the option described above.
- **Number of events with symbol** - Allow a tick(hit) if **X** events with the specific symbol are provided. For example, if you enter 10, a tick will be counted for every 10 installation of a certain software. **Applies when number of events** - Enter a number of events in a row after the last tick to count another tick. For example, enter 10 and a tick will be counted after 10 events from the last tick.
- **Applies when number of events** - The trigger is applied when the ticks are either **Received in a Row** (trigger execution is not taken into account), or **Received Since Last Trigger Execution** (when the trigger is executed, the number is reset to 0).

Distribution

Subject - Subject of the message that contains the notification. This is optional, but also recommended for better filtering or when creating rules to sort the messages.

Distribution

- **Send SNMP Trap** - Sends an SNMP Trap. The SNMP Trap notifies the Server using an unsolicited SNMP message. For more information, see How to configure an SNMP Trap Service.
- **Send email** - Sends an email message based on your email settings.

Email addresses - Enter the email addresses of the recipients of the notification messages, separate multiple addresses with a comma (","**,**").

6.1.5.3 How to configure an SNMP Trap Service

To successfully receive SNMP messages, the SNMP trap service needs to be configured.

Configuration steps according to operating system

- Windows
- Linux

WINDOWS

Prerequisites

- The **Simple Network Management Protocol** service must be installed on the machine where ERA Server is installed, as well as the machine where the SNMP trap software will be installed.
- Both computers (above) should be in the same subnet.
- The SNMP Service must be configured on the ERA Server computer.

SNMP Service configuration (ERA Server)

- Press the Windows key + R to open a run dialog box, type *Services.msc* into the **Open** field and press **Enter**. Search for the SNMP Service.
- Open the **Traps** tab, type **public** into the **Community name** field and click **Add to list**.
- Click **Add,** type the **Host name, IP** or **IPX address** of the computer where the SNMP trapping software is installed into the appropriate field and click **Add**.
- Proceed to the **Security** tab. Click **Add** to display the **SNMP Service Configuration** window. Type **public** into the **Community name** field and click **Add**. Rights will be set to **READ ONLY**, this is ok.
- Make sure that **Accept SNMP packets from any hosts** is selected and click **OK** to confirm. The SNMP service is not configured.

SNMP Trap Software configuration (Client)

- The SNMP Service is installed and doesn`t need to be configured.
- Install **AdRem SNMP Manager** or **AdRem NetCrunch**.
- **AdRem SNMP Manager**: Start the application and select **Create New SNMP Node List.** Click **Yes** to confirm.
- Check the network address of your subnet (displayed in this window). Click **OK** to search your network.
- Wait for the search to finish, the search results will be displayed in the **Discovery results** window. The IP address of the ERA Server should be displayed in this list.
- Select the IP address of the server and click **OK**. Your server address is displayed in the **Nodes** section.
- Click **Trap Receiver Stopped** and select **Start**. **Trap Receiver Started** will be displayed. Now you can receive SNMP messages from your ERA Server.

LINUX

1. Install the snmpd package by running one of the following command:
   `apt-get install snmpd snmp` (Debian, Ubuntu distributions)
   `yum install net-snmp` (Red-Hat, Fedora distributions)

2. Open the */etc/default/snmpd* file and make the following attribute edits:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```
Adding # will disable this line completely.

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
```
Add this line to the file.

```
TRAPDRUN=yes
```
Change the *trapdrun* attribute to *yes*.

3. Create a backup of the original *snmpd.conf* file. The file will be edited later.

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. Create a new *snmpd.conf* file and add these lines:

```
rocommunity public
syslocation "Testing ERA6"
syscontact admin@ERA6.com
```

5. Open the */etc/snmp/snmptrapd.conf* file and add the following line at the end of the file:

```
authCommunity log,execute,net public
```

6. Type the following command to start the SNMP manager services and logging of incoming traps:

```
/etc/init.d/snmpd restart
```
or
```
service snmpd restart
```

7. To check if the trap is working and catching the messages, run the following command:

```
tail -f /var/log/syslog | grep -i TRAP
```

6.1.6 Certificates

A certificate authenticates the data exchanged in communications between the ERA Server and the Agent because the ERA Server communicates through an Agent as well.

- Create a new Certificate using the ERA Certification Authority
- Create a new Certificate using a custom Certification Authority
- Create a new Certificate Authority

6.1.6.1 Peer Certificates

A certificate authenticates the data in communication between the ERA Server and the Agent because the ERA Server communicates through an Agent as well.

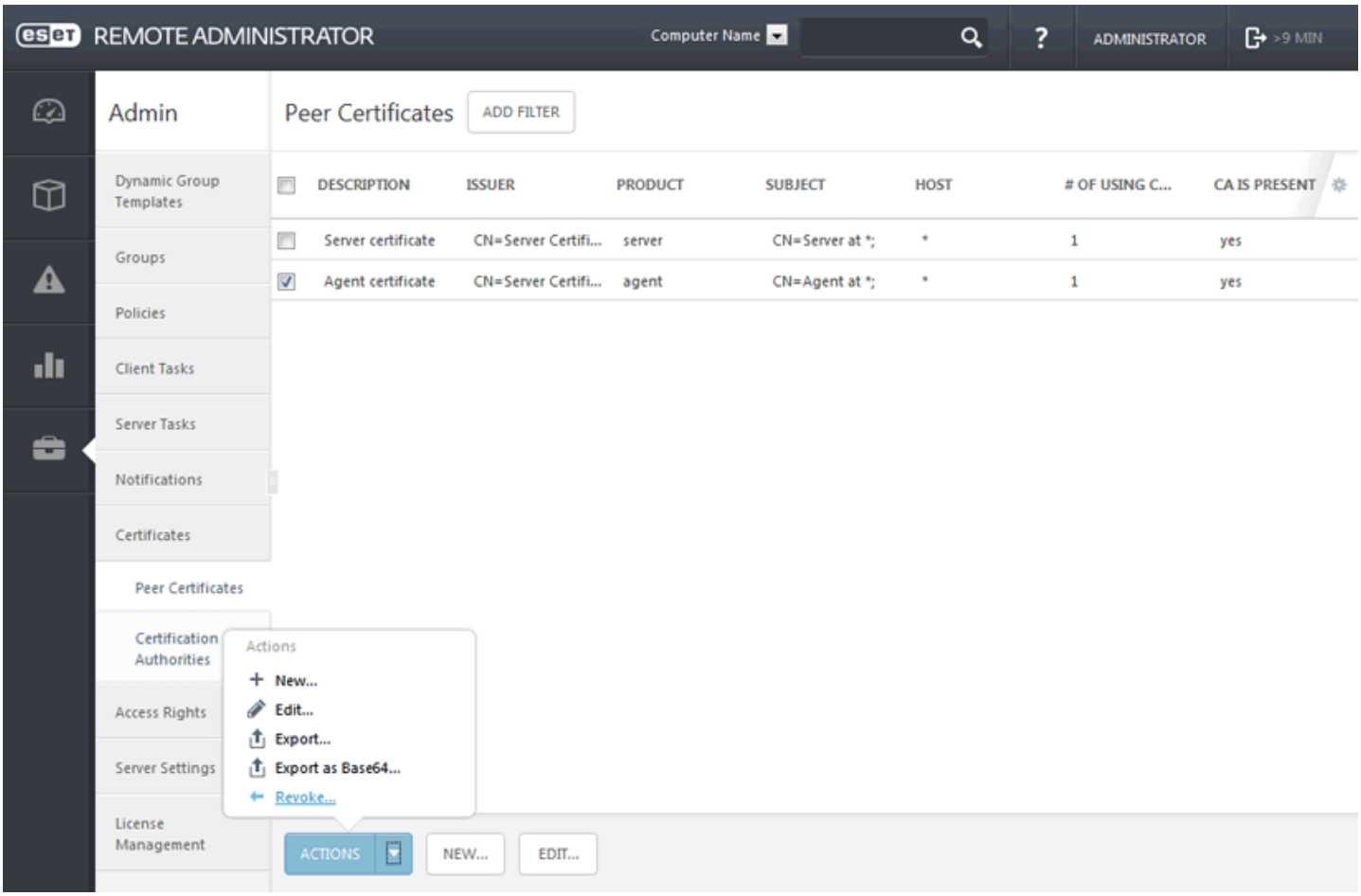
+ New... - This option is used to create a new certificate using the ERA Certification Authority or create a new Certificate using a custom Certification Authority. These certificates are used for the Agent, Proxy and Server.

Edit... - Select this option to edit an existing certificate from the list. The same options apply as when you create a new certificate.

Export... - This option is used to export the certificate as a file. This file is necessary if you install the Agent locally on a computer or when installing Mobile Device Connector.

Export as Base64... - This option is used to export the certificate as a .txt file.

Revoke... - If you no longer want to use a certificate, select **Revoke**. This option invalidates the certificate. Invalid certificates will not be accepted by ESET Remote Administrator.

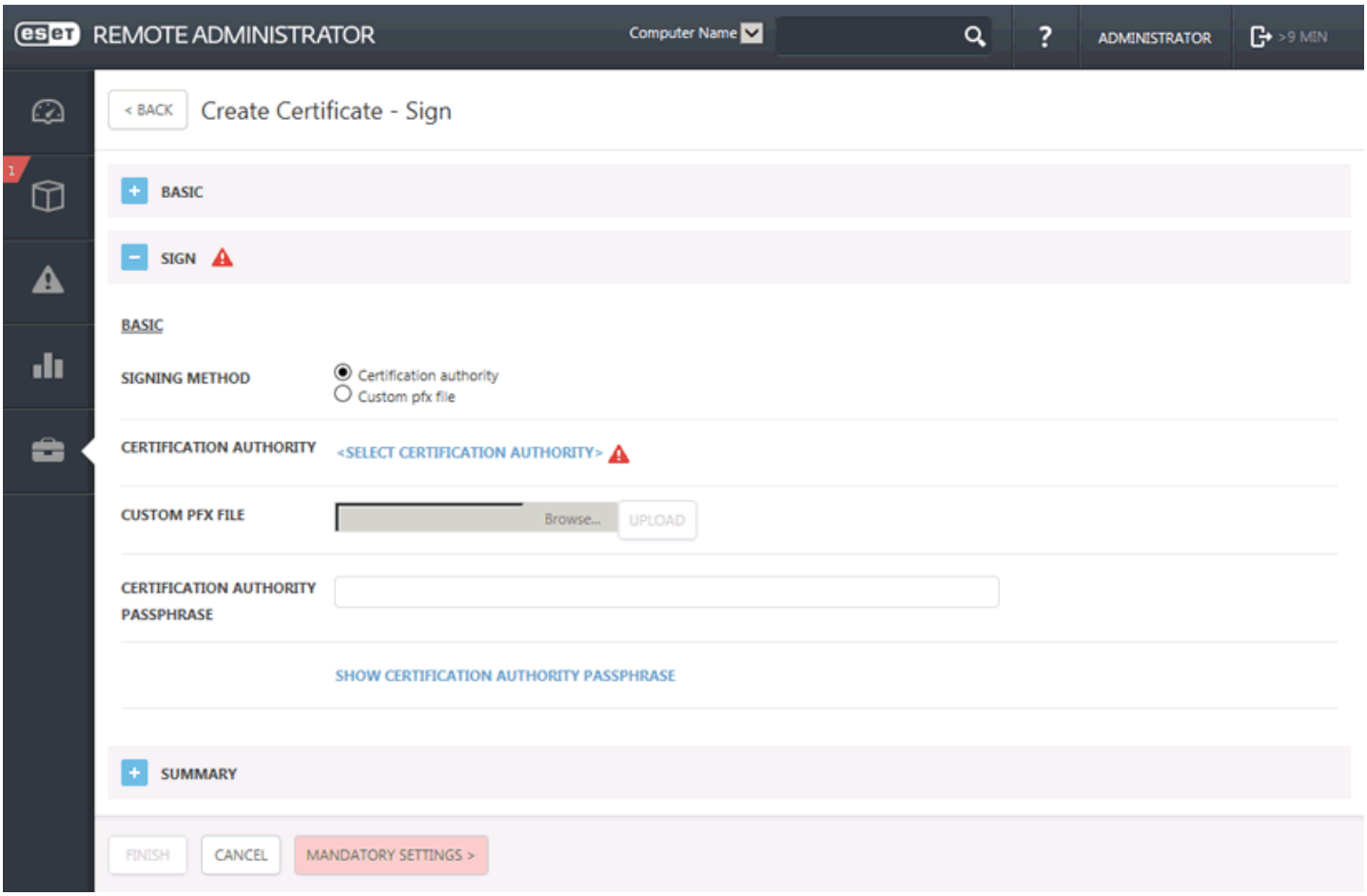


6.1.6.1.1 Create a new Certificate using the ERA Certification Authority

To create a new authority in the **ERA Web Console**, navigate to **Admin** > **Certificates** and click **Actions** > **New**.

Basic

- Enter a **Description** for the certificate and select **Agent** as the **Product**.
- Enter a connection to the ERA Server in the **Host** field. It can be a hostname, an IP Address or a partial name with a wildcard ("*"). Multiple entries are separated using a space (" "), comma (",") or semicolon (";").
- Enter a password into the **Passphrase** field and confirmation field. This password will be used during Agent installation.
- Type a value into the **Common name** field. This value should contain the string "Agent", "Proxy" or "Server", according to the selected **Product**.
- If you want, you can enter descriptive information about the certificate.
- Enter the **Valid from** and **Value to** values to ensure that the certificate is valid.



Sign

- The signing method should be **Certification authority**.
- Select the **ERA Certificate Authority** created during the initial installation.
- Skip the custom `pfx` file option, this option only applies to self-signed `pfx` certification authorities.
- Enter the password for the certificate, this password is the **Certification authority passphrase** created during Server Installation.

Summary

- Review the certificate information you entered and click **Finish**. The certificate is now successfully created and will be available in the **Certificates** list to use when installing the Agent.

6.1.6.1.2 Create a new Certificate using a custom Certificate Authority

To create a new authority in the **ERA Web Console**, navigate to **Admin** > **Certificates** and click **Actions** > **New**.

Basic

- Enter a **Description** for the certificate and select **Agent** as the **Product**.
- Enter a connection to the ERA Server in the **Host** field. It can be a hostname, an IP Address or a partial name with a wildcard ("*"). Multiple entries are separated using a space (" "), comma (",") or semicolon (";").
- Enter a password into the **Passphrase** field and confirmation field. This password will be used during Agent installation.
- Type a value into the **Common name** field. This value should contain the string "Agent", "Proxy" or "Server", according to the selected **Product**.
- If you want, you can enter descriptive information about the certificate.
- Enter the **Valid from** and **Value to** values to ensure that the certificate is valid.

Sign

- The signing method should be **Custom pfx file**.
- Click **Browse** to select a custom `pfx` file. Navigate to your custom `pfx` file and click **OK**. Click **Upload** to upload this certificate to the Server.
- Enter the password for the certificate, this password is the **Certification authority passphrase** created during Server Installation.

Summary

- Review the certificate information you entered and click **Finish**. The certificate is now successfully created and can be used to install the Agent.

6.1.6.2 Certificate Authorities

In the **Certificate Authorities** section, the Certificate Authorities are listed and managed. If you have multiple Certificate Authorities, it might be useful to apply a filter to sort them.

Click **Add Filter** at the top of the page and select the filtering criteria you want to use (**Description**, **Subject**, **Valid From/To**, etc.). You can set one criteria per filter. Once you select one of the criteria and click **OK** a text field opens next to the **Add Filter** button. You can enter custom information into this text field, such as a **Date** and **Description**. To create an additional filter click **Add Filter**, you can create as many filters as you want.

6.1.6.2.1 Create a new Certificate Authority

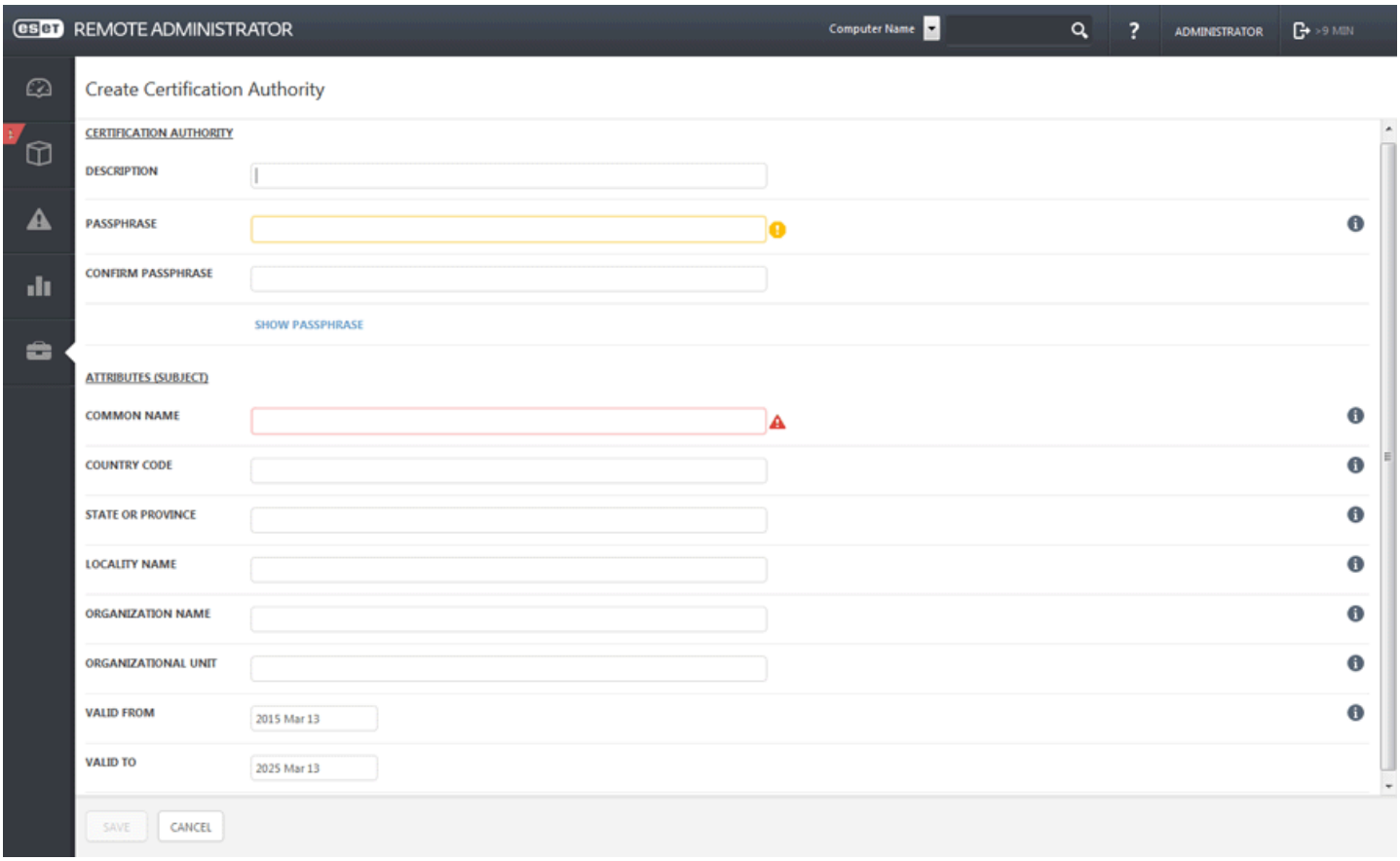
To create a new authority, navigate to **Admin** > **Certificates** > **Certification Authority** and click **Action** > **+ New...**, or **New** at the bottom of the page.

Certification Authority

Enter a **Description** of the Certification Authority and select a **Passphrase**. This **Passphrase** should contain at least 12 characters.

Attributes (Subject)

1. Enter a **Common name** (name) of the Certification Authority. Select a unique name to differentiate multiple Certificate Authorities.
   Optionally, you can enter descriptive information about the Certificate Authority.
2. Enter the **Valid from** and **Valid to** values to ensure that the certificate is valid.
3. Click **Save** to save your new Certification Authority. It will now be listed in the Certification Authority list under **Admin** > **Certificates** > **Certification Authority**, and is ready to be used.



To manage the Certificate Authority, select the check box next to the Certification Authority in the list and use the contact menu (left-click the Certificate Authority) or the **Action** button on the bottom of the page. Available options are **Edit** the Certification Authority (see the steps above), **Delete** it completely or **Export a public key**.

Export a public key from a Certificate Authority

1. Select the Certification Authority you want to use from the list and select the check box next to it.
2. From the context menu select **Export Public Key**. The public key will be exported as a *.der* file. Select a name for the public key and click **Save**.

NOTE: If you delete the default ERA Certification Authority and create a new one, it will not work. You also need to assign it to ERA Server machine and restart the ERA Server service.

6.1.7 Access Rights

Access Rights in ERA can be divided into two basic categories:

1. Functionality access
2. Static group access

Access to the items from either category must be granted to every User of ERA Web Console permissions.

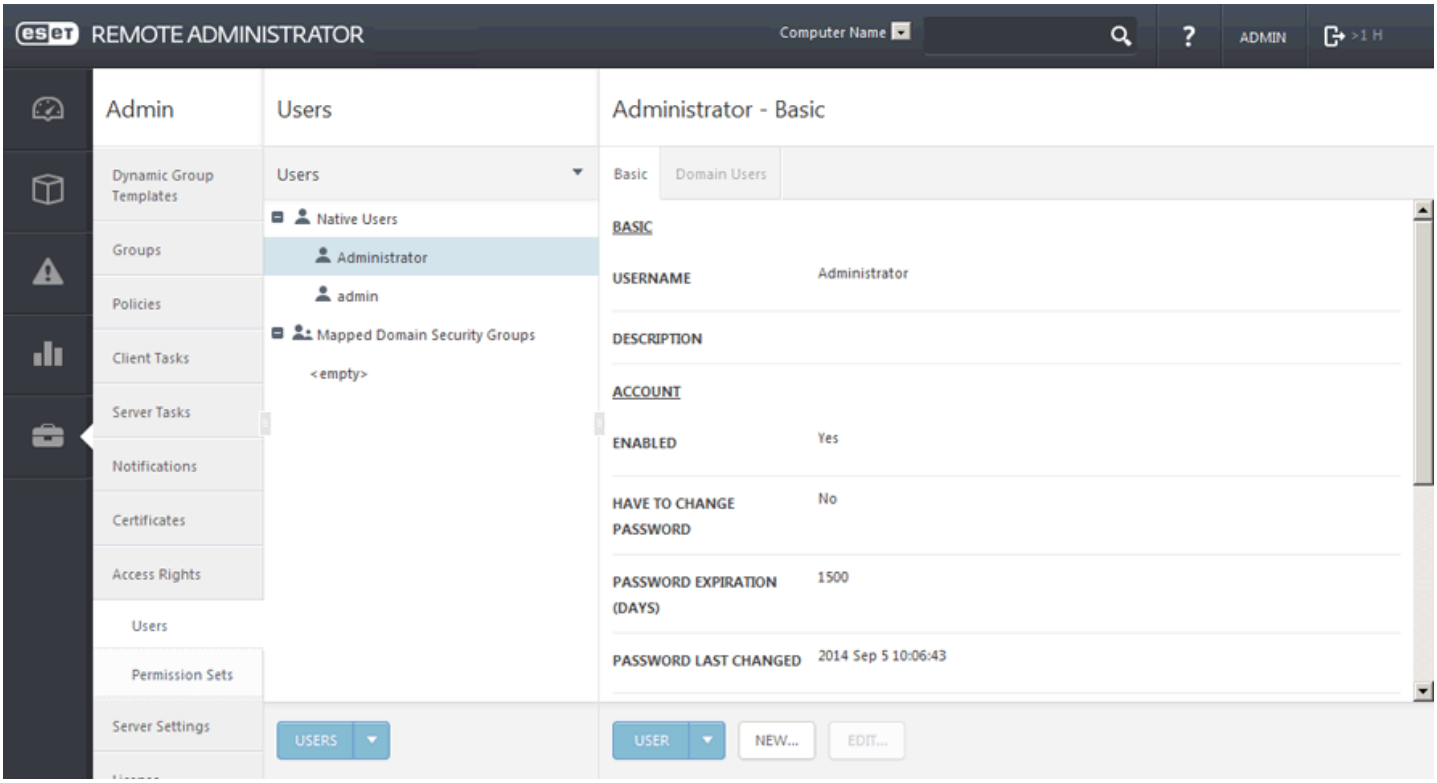
On the top is **Administrator** user with access to everything. Because of too many competences using this account may rather be dangerous. It is **strongly advised** to create further accounts with narrower access rights based on account desired competences.

Users are managed in Users area of the Admin section. Their possible competences are represented by Permission Sets.

6.1.7.1 Users

ERA Web Console can have users of various permission sets. The user with the most permissions is the **Administrator**, with full rights and permissions. To ease usage in Active Directory, users from **Domain security groups** can be allowed to log into ERA. Such users can exist next to ERA **Native Users**, however, the permission sets are set for the Active Directory security group (instead of for individual users, as in the **Native User** case).

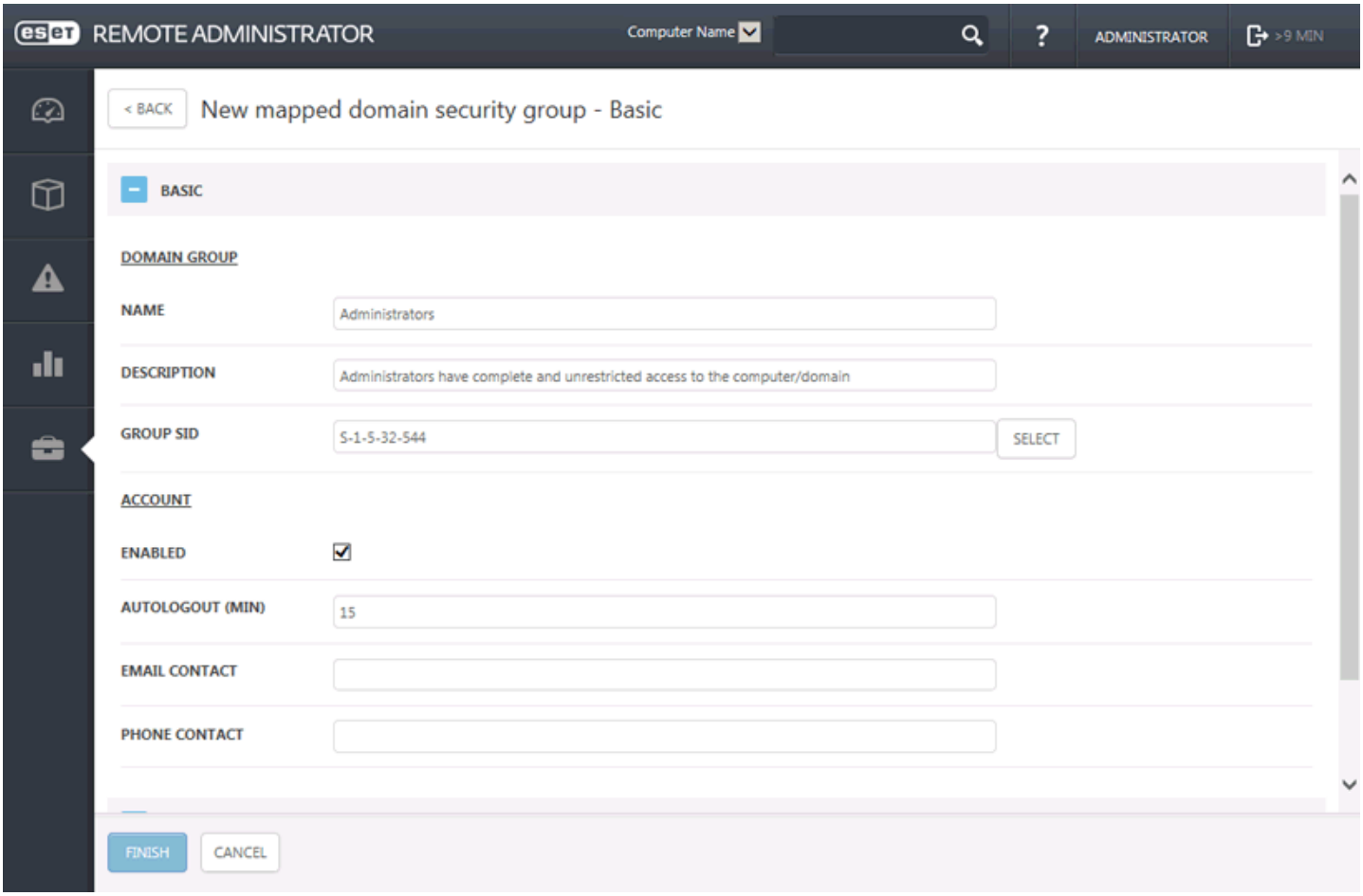
User management is part of the **Admin** section of the ERA Web Console.



NOTE: A fresh ERA installation has the **Administrator** (**Native User**) as the only account.

6.1.7.1.1 Mapped Domain Security Group Wizard

To acccess the **Mapped Domain Security Group Wizard**, navigate to **Admin** > **Access Rights** > **Mapped domain security groups** > **New** or simply **New** (when the mapped domain security group is selected in the tree).



Basic

Domain group

Enter a **Name** for the group, you can also enter a group **Description**. The group will be defined by a **Group SID** (security identifier). Click **Select** to select a group from the list and then click **OK** to confirm.

Account

- Leave **Enabled** selected to make the user active.
- The **Autologout (min)** option defines the idle time period (in minutes), after which the user is logged out of the ERA Web Console.
- **Mail contact** and **Phone Contact** are optional and can be used to identify the user.

Permission set

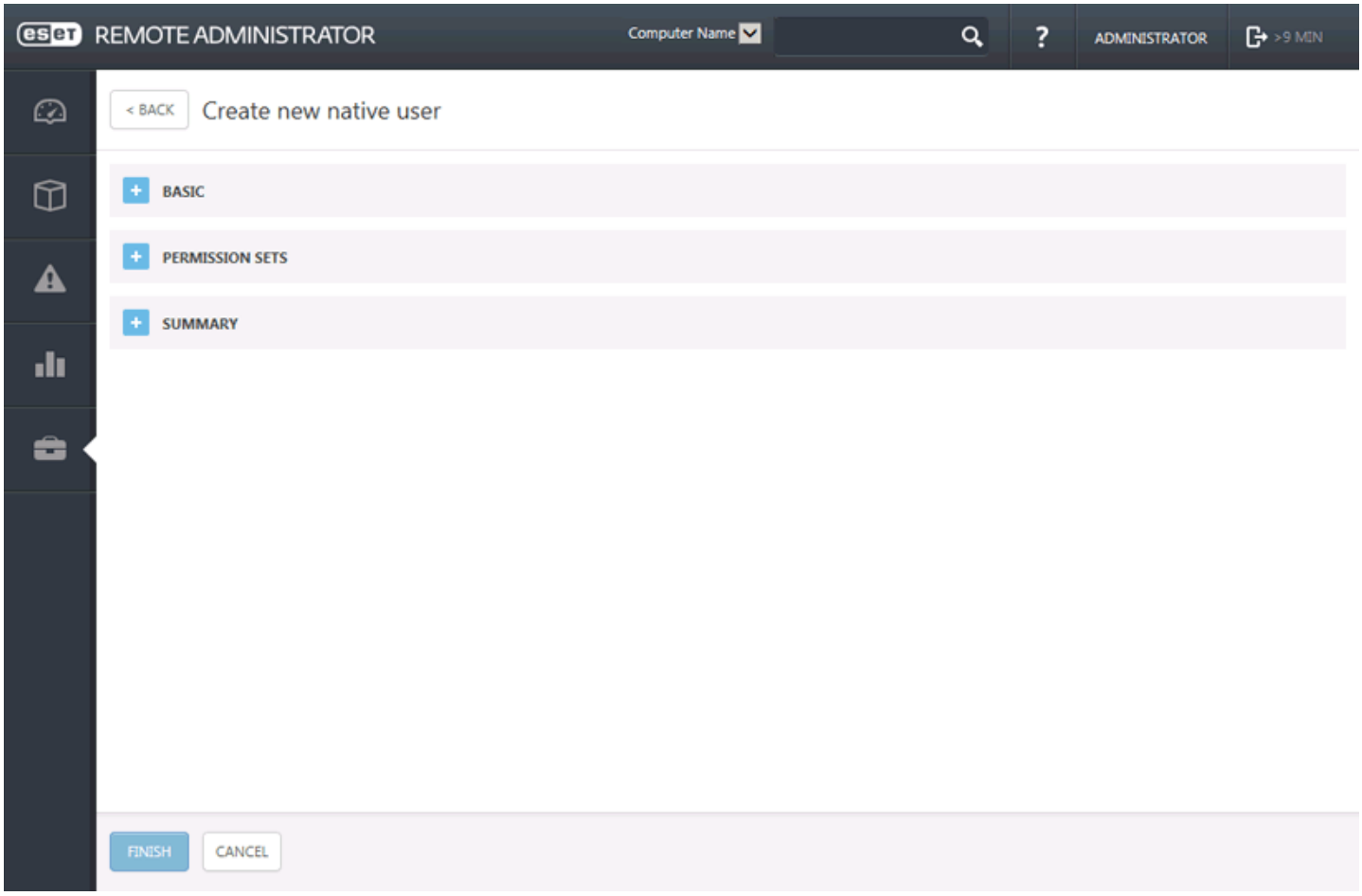
Assign competences (rights) for the user. You can use a pre-defined competence: **Reviewer permission set** (similar to read-only rights) or **Administrator permission set** (similar to full access), or you can use a custom permission set.

Summary

Review the settings configured for this user and click **Finish** to create the group.

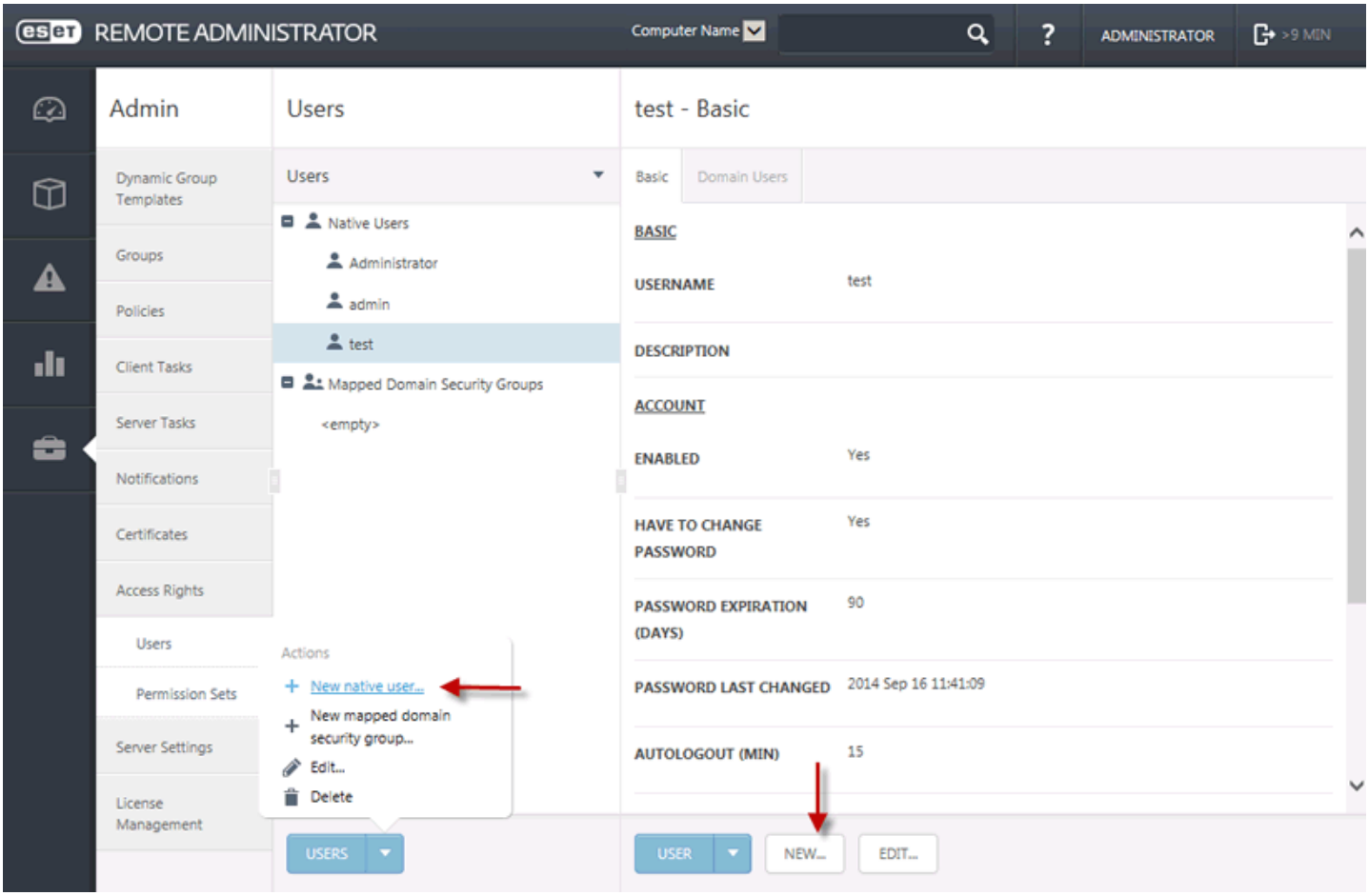
6.1.7.1.2 Native User Wizard

To access the **Native User Wizard**, navigate to **Admin** > **Access Rights** > **User** > **Users** or **New** on the bottom of the page.



6.1.7.1.3 Create a Native User

To create a new Native User, from the **Admin** tab click **Access Rights** > **User** and then click **Users** or **New** at the bottom of the page.



Basic

Enter a **Username** and an optional **Description** for the new user.

Authentication

The password for the user should have at least 8 characters. The password should not contain the username.

Account

- Leave **Enabled** selected unless you want the account to be inactive (if you intend to use it later).
- Leave **Have to change password** deselected (selecting this will force the user to change their password the first time that they log into the ERA Web Console).
- The **Password expiration** option defines the number of days that the password is valid, it needs to be changed after that.
- The **Autologout(min)** option defines the idle time period (in minutes), after which the user is logged out of Web Console.
- **Full Name**, **Email contact** and **Phone contact** can be defined to help identify the user.

Permission set

Assign competences (rights) for the user. You can select a pre-defined competence: **Reviewer permission set** (similar to read-only rights) or **Administrator permission set** (similar to full access), or you can use a custom permission set.

Summary

Review the settings configured for this user and click **Finish** to create the account.

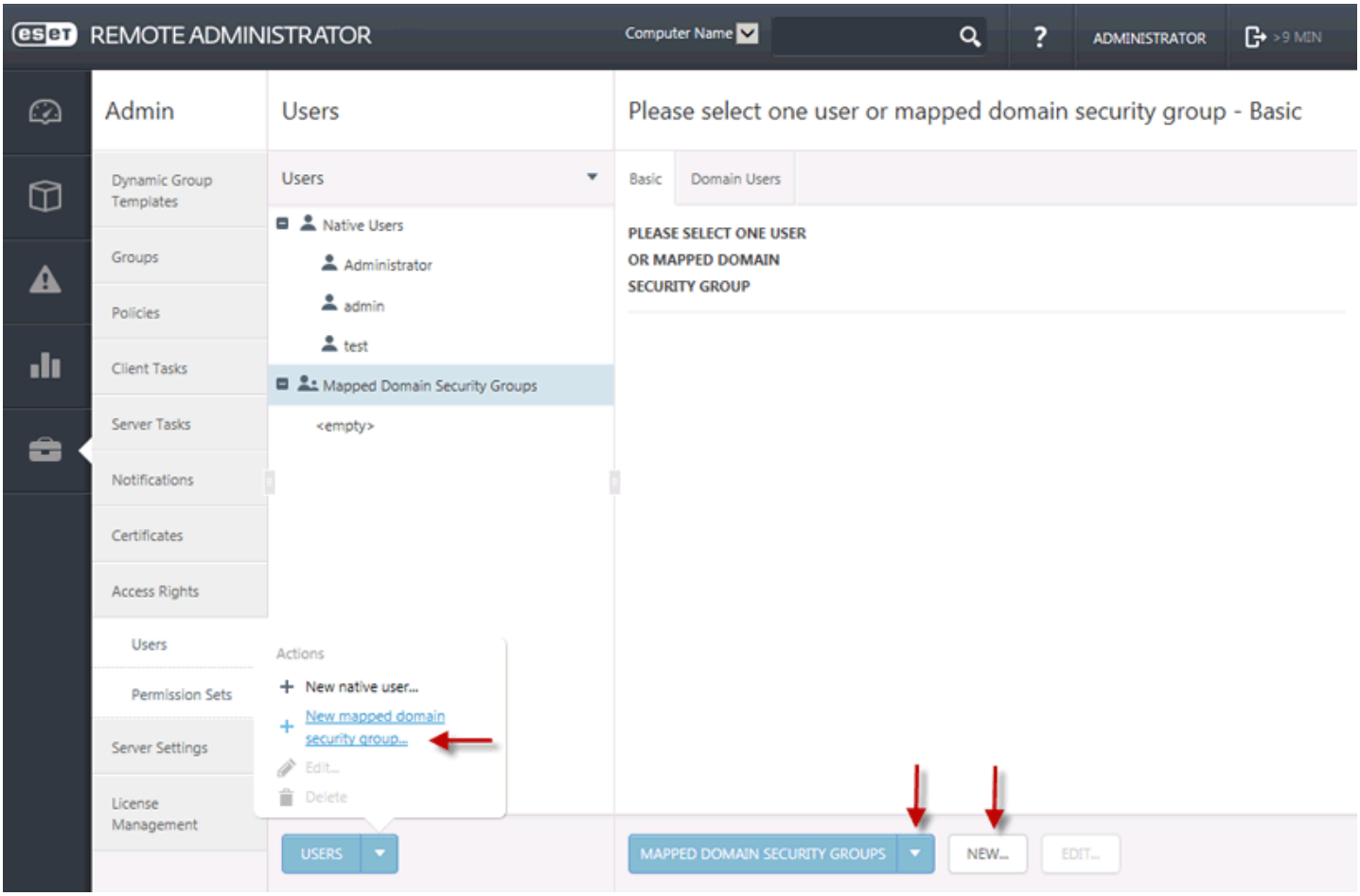
6.1.7.1.3.1 Create New Admin account

To create a second Administrator account, follow steps to create a native user account and assign the Administrator permission set to this account.

6.1.7.1.4 Map Group to Domain Security Group

You can map a domain security group to the ERA Server and allow existing users (members of these domain security groups) to become ERA Web Console users.

Click **Admin** > **Access Rights** > **Mapped domain security groups** > **New** or simply **New** (when the mapped domain security group is selected in the tree).



Basic

Domain group

Enter a **Name** for the group, you can also enter a group **Description**. The group will be defined by a **Group SID** (security identifier). Click **Select** to select a group from the list and then **OK** to confirm.

Account

- Leave **Enabled** selected to make the user active.
- The **Autologout (min)** option defines the idle time period (in minutes), after which the user is logged out of the Web Console.
- **Mail contact** and **Phone Contact** are optional and can be used to identify the user.

Permission set

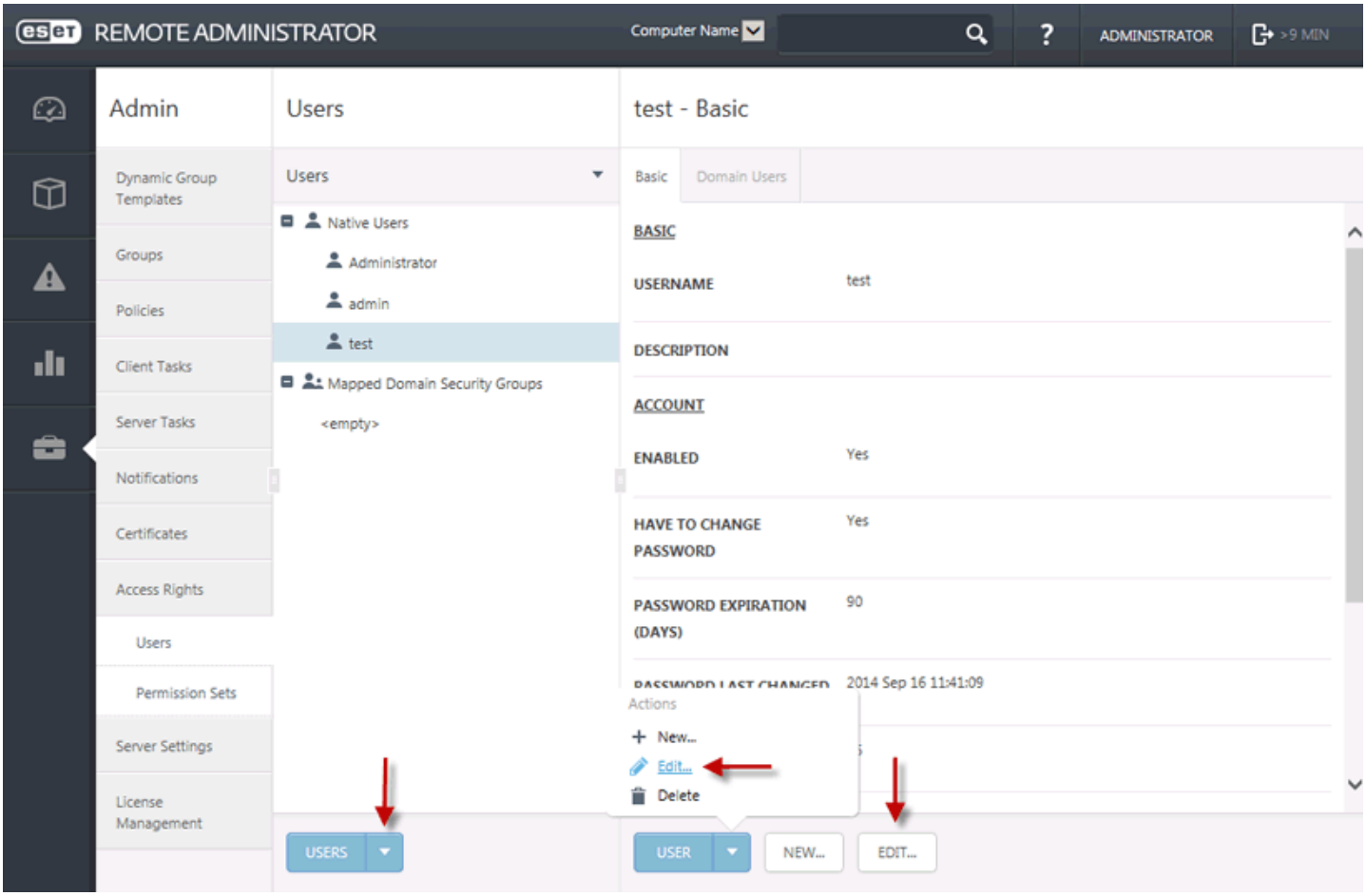
Assign competences (rights) for the user. You can use a pre-defined competence: **Reviewer permission set** (similar to read-only rights) or **Administrator permission set** (similar to full access), or you can use a custom permission set.

Summary

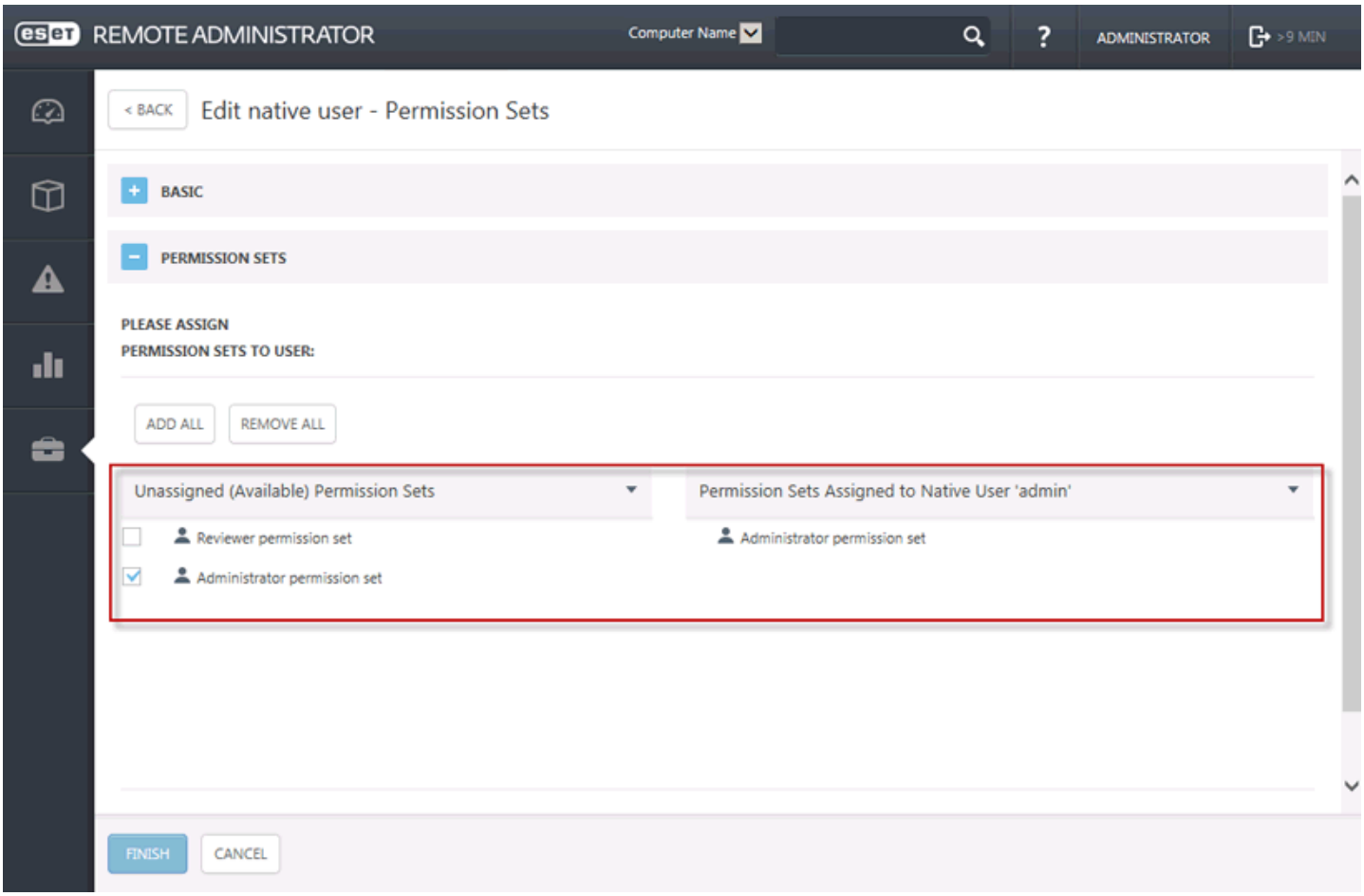
Review the settings configured for this user and click **Finish** to create the group.

6.1.7.1.5 Assign User a Permission Set

Admin > **Access rights** > **Permission Sets** and then click **Edit** to assign a user to a specific permission set. See Manage PermissionSets for more details.



In the **Users** section, edit a specific user by clicking **Edit...** and select the check box next to a specific permission set in the **Unassigned (Available) Permission Sets** section.



6.1.7.2 Permission Sets

A permission set represents the permissions for users that access ERA Web Console, they define what the user can do or see in the Web Console. Native users have their own permissions while domain users have the permissions of their mapped security group.

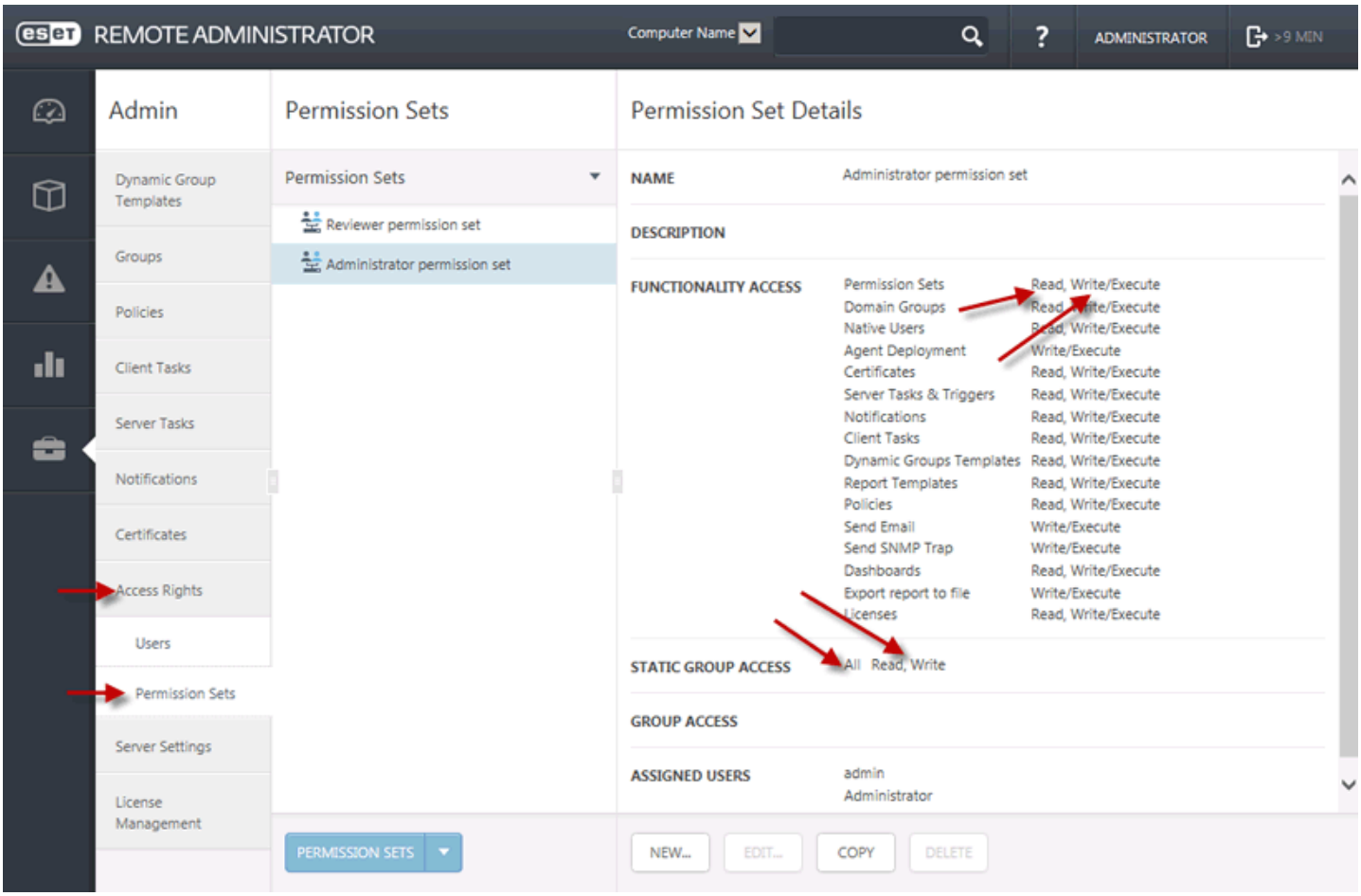
ERA Web Console permissions are divided into categories, for example, Native Users, Certificates, Policies and so on. For each functionality, a given permissions set can allow for **Read-only** or **Write/Execute** access.

Read-only permissions are good for auditing users. They can view data but cannot make changes.

Write/Execute allows users with this privilege to either modify respective objects or execute them (when possible - for instance Tasks can be executed).

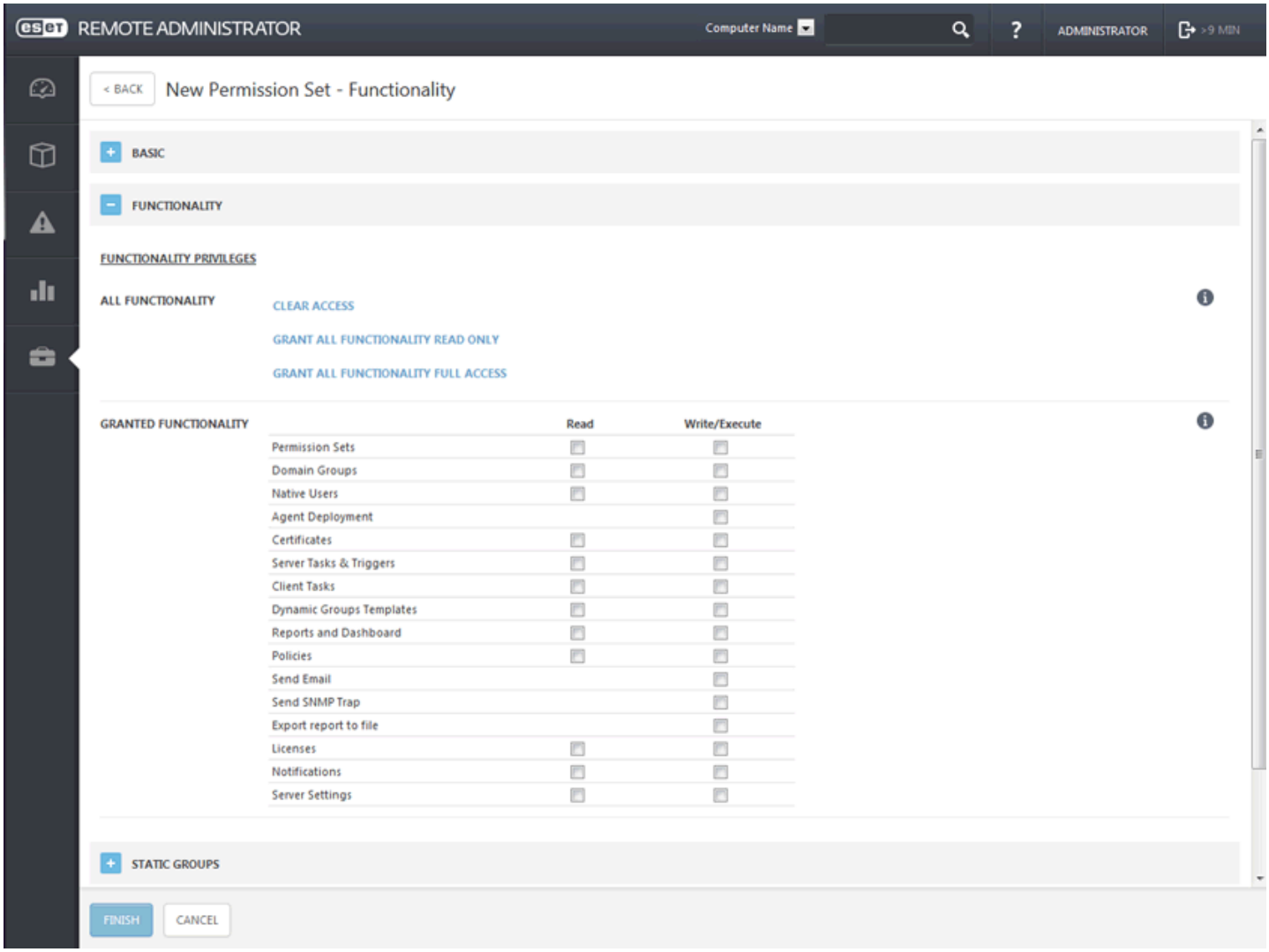
Next to permissions to ERA functionality, there can be give access to Static Groups. Every user can be given access to either **all** or to **subsets of Static Groups**. Having access to certain Static Group automatically means access to every of its subgroups. In this case:

- **Read-only** access means listing of computers.
- **Write/Execute** permission gives user ability to manipulate computers in the Static Group, as well as assign Client Tasks and Policies.


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
>9 MIN
Admin
Dynamic Group Templates
Groups
Policies
Client Tasks
Server Tasks
Notifications
Certificates
Access Rights
Users
Permission Sets
Server Settings
License Management
Permission Sets
Permission Sets
Reviewer permission set
Administrator permission set
PERMISSION SETS
Permission Set Details
NAME
Administrator permission set
DESCRIPTION
FUNCTIONALITY ACCESS
Permission Sets Read, Write/Execute
Domain Groups Read, Write/Execute
Native Users Read, Write/Execute
Agent Deployment Write/Execute
Certificates Read, Write/Execute
Server Tasks & Triggers Read, Write/Execute
Notifications Read, Write/Execute
Client Tasks Read, Write/Execute
Dynamic Groups Templates Read, Write/Execute
Report Templates Read, Write/Execute
Policies Read, Write/Execute
Send Email Write/Execute
Send SNMP Trap Write/Execute
Dashboards Read, Write/Execute
Export report to file Write/Execute
Licenses Read, Write/Execute
STATIC GROUP ACCESS
All Read, Write
GROUP ACCESS
ASSIGNED USERS
admin
Administrator
NEW...
EDIT...
COPY
DELETE

6.1.7.2.1 Permission Set Wizard

To add a new permission set, click **Permissions sets** > **New** or simply **New**.

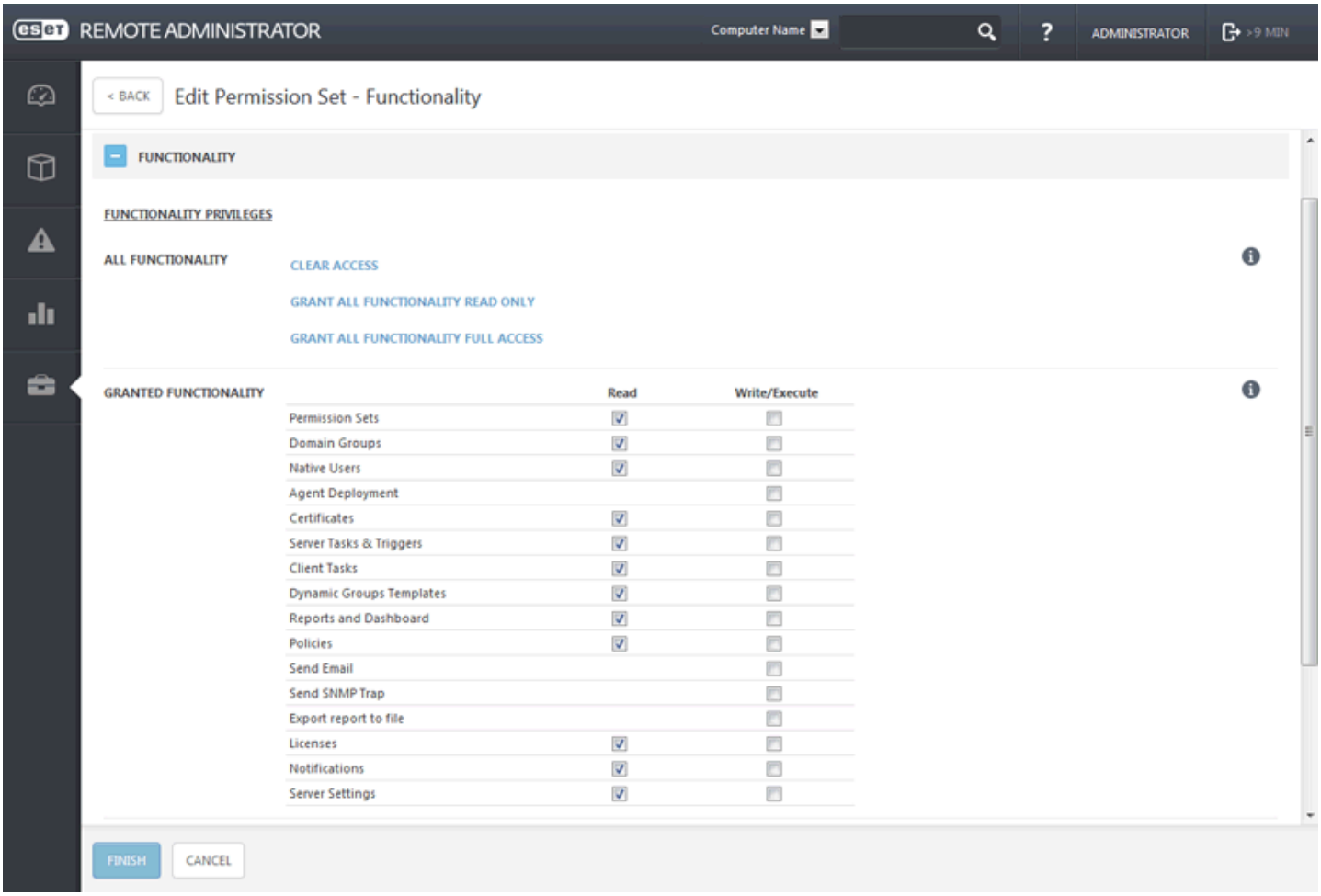


6.1.7.2.2 Manage Permission Sets

To make changes to a specific permissions set, click it and then click **Edit**. Click **Copy** to create a duplicate permission set which you can modify and assign to a specific user.

Basic

Enter a **Name** for the set (mandatory setting), you can also enter a set **Description**.



Functionality

Select individual modules for which you want to grant access. The User with this competence will have access to these specific tasks. It is also possible to **Grant all modules read-only** and **Grant all modules full access**, but such competences already exist - **Administrator competence** (full access) and **Reviewer competence** (read only). Granting **Write/Execute** rights automatically grants **Read** rights.

Static groups

You can add a Static Group (or multiple Static Groups) that will take this competence (and take over the rights defined in the **Modules** section), grant all Static Groups read-only access or grant all Static Groups full access. You can only add Static Groups, because the granted permissions sets are fixed for certain users or groups.

Users

All available users are listed on the left. Select specific users or select all users using the **Add All** button. Assigned users are listed on the right.

Summary

Review the settings configured for this competence and click **Finish**.

6.1.8 Server Settings

In this section, you can configure specific settings for the ESET Remote Administrator Server itself.

Connection

- **Remote Administrator port (requires restart!)** - This is the port for the connection between the ESET Remote Administrator Server and the Agent(s). Changing this option requires restarting the ERA Server Service before the change takes effect.
- **ERA Web Console port (requires restart!)** - Port for the connection between the Web Console and the ERA Server.
- **Certificate** - Here you can manage certificates. For more information, see the chapter Peer Certificates.

Updates

- **Update interval** - Interval on which the updates will be received. You can select a regular interval and configure the settings, or you can use a CRON expression.
- **Update server** - Update server from which the ERA Server receives updates for security products and ERA Components.
- **Update type** - Select the type of updates you want to receive. Either regular, pre-release or delayed updates. We do not recommend that you select the pre-release option for production systems as this is a risk.

Advanced Settings

- **HTTP Proxy** - You can use a proxy server to allow connection to the internet.
- **SMTP Server** - You can use an SMTP Server to receive or send different messages. Here you can configure settings for your SMTP server.
- **Repository** - Location of the repository where all installation files are stored.
- **Logging** - You can set the log verbosity that determines the level of information that will be collected and logged - from **Trace** (informational) to **Fatal** (most important critical information).
- **Database cleanup** - To prevent a database overload, you can use this option to regularly clean logs.

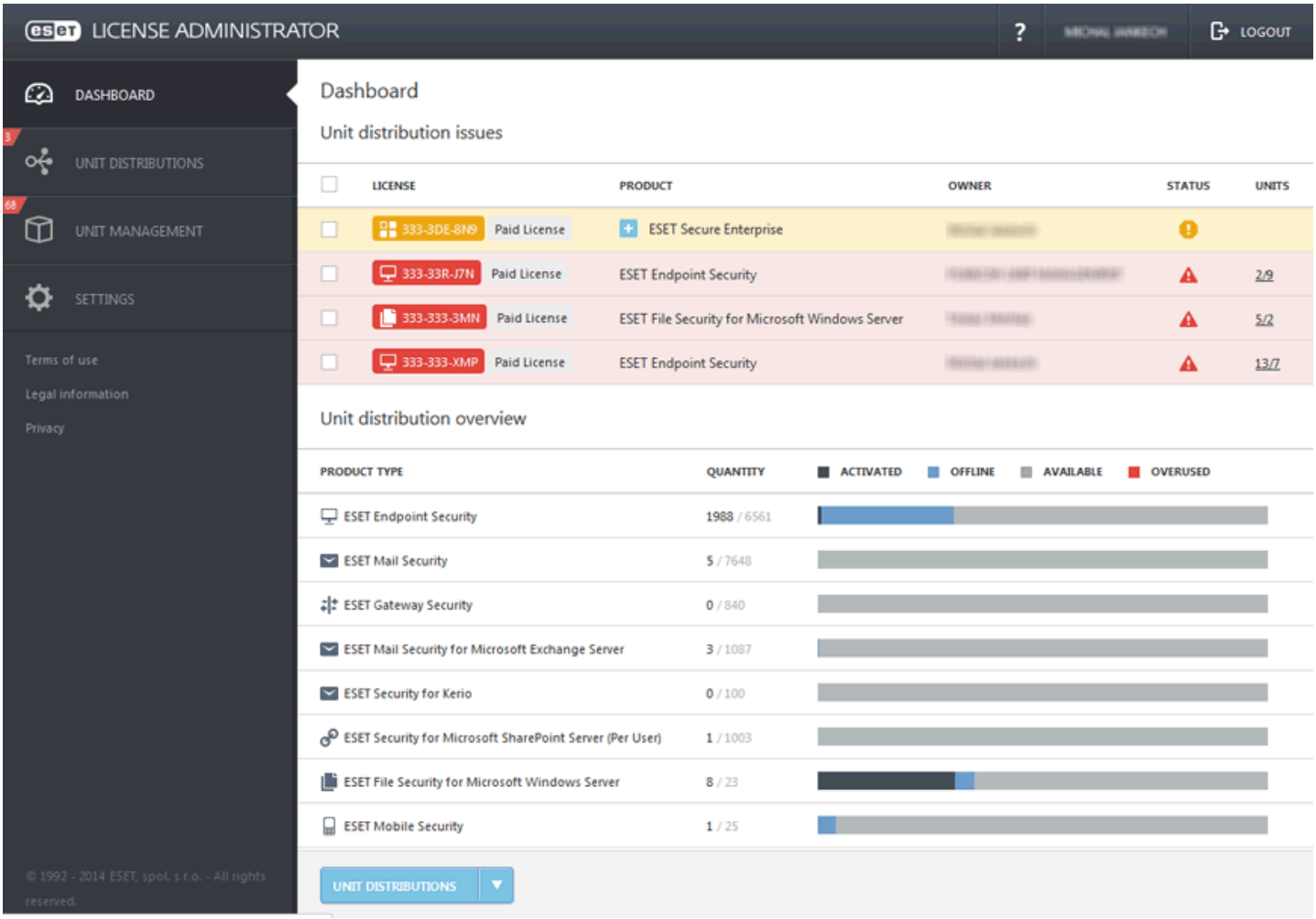
6.1.9 License Management

ESET Remote Administrator from version 6 uses a completely new ESET licensing system.

The username and the password are replaced by a **License Key/Public ID** - a **License Key** is a unique string which is used to identify the license owner and the activation itself. The **Public ID** is a short string used to identify the license by a 3rd party (for example, the **Security Admin** responsible for the Unit distribution).

A **Security Admin** is a person who manages the licenses and can be different from the actual **License Owner**. The license owner can delegate a license to a security admin (authorize him) and if he accepts, he can manage it (make changes, associate units, etc.). A security admin can use the license to activate ESET products (associate a unit).

Licenses can be managed either from this section, or online by clicking either **Open ELA** (ESET License Administrator) or using the ESET License Administrator web interface (see the Security Admin section).



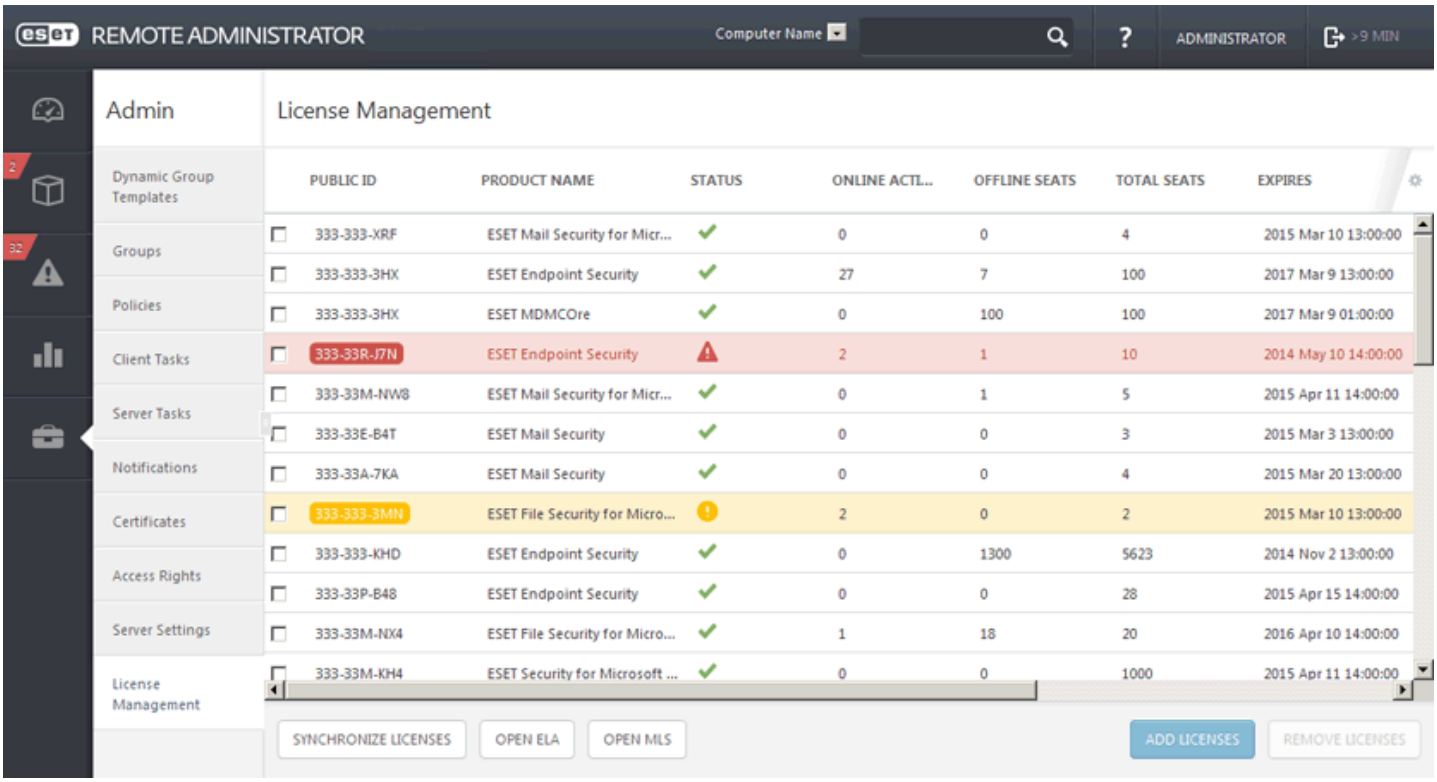
The License Management section in ESET Remote Administrator 6 is accessible from the main menu under **Admin** > **License Management**.

Licenses can be distributed to ESET security products from ERA using two tasks:

- The Software installation task
- The Product activation task

Licenses are uniquely identified by their public ID. Each license displays:

- the security **Product name** for which its license is intended
- the overall **Status** of the license (if the license is expired, overused, or at risk of expiration or overuse, a warning message will be displayed here)
- the number of **Units** that can be activated with this license
- the license expiration date
- the license **Owner name** and **Contact**.


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
>9 MIN
Admin
License Management
Dynamic Group Templates
Groups
Policies
Client Tasks
Server Tasks
Notifications
Certificates
Access Rights
Server Settings
License Management
PUBLIC ID
PRODUCT NAME
STATUS
ONLINE ACTI...
OFFLINE SEATS
TOTAL SEATS
EXPIRES
333-333-XRF ESET Mail Security for Micr... 0 0 4 2015 Mar 10 13:00:00
333-333-3HX ESET Endpoint Security 27 7 100 2017 Mar 9 13:00:00
333-333-3HX ESET MDMCOre 0 100 100 2017 Mar 9 01:00:00
333-33R-J7N ESET Endpoint Security 2 1 10 2014 May 10 14:00:00
333-33M-NW8 ESET Mail Security for Micr... 0 1 5 2015 Apr 11 14:00:00
333-33E-B4T ESET Mail Security 0 0 3 2015 Mar 3 13:00:00
333-33A-7KA ESET Mail Security 0 0 4 2015 Mar 20 13:00:00
333-333-3MN ESET File Security for Micro... 2 0 2 2015 Mar 10 13:00:00
333-333-KHD ESET Endpoint Security 0 1300 5623 2014 Nov 2 13:00:00
333-33P-B48 ESET Endpoint Security 0 0 28 2015 Apr 15 14:00:00
333-33M-NX4 ESET File Security for Micro... 1 18 20 2016 Apr 10 14:00:00
333-33M-KH4 ESET Security for Microsoft ... 0 0 1000 2015 Apr 11 14:00:00
SYNCHRONIZE LICENSES
OPEN ELA
OPEN MLS
ADD LICENSES
REMOVE LICENSES

Synchronize licenses

License synchronization with ESET License Administrator happens automatically once a day. If you make changes in ESET License Administrator and want current license information to appear in ERA right away instead of waiting for next automatic synchronization, click **Synchronize licenses** button.

Add License or License key

Click **Add Licenses** and then select the method you want to use to add your new license(s):

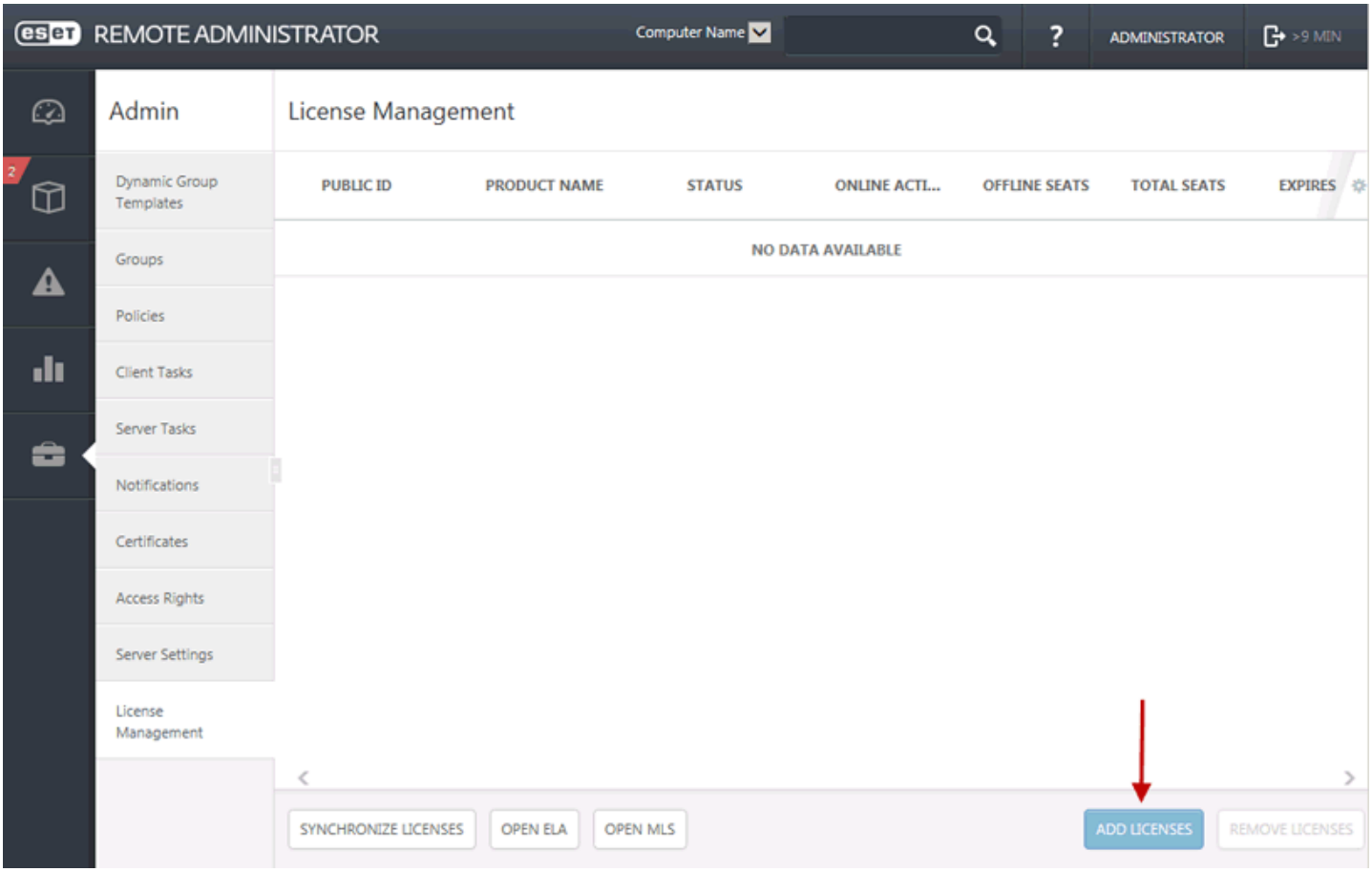
1. License Key - Enter a license key for a valid license and click **Add License**. The license key will be verified against the activation server and added to the list.
2. Security Admin Credentials - Connect a security admin account and all its licenses to the **License Management** section.
3. License File - Add a license file (.lf) and click **Add License**. The license file will be verified and the license added to the list.

Remove Licenses

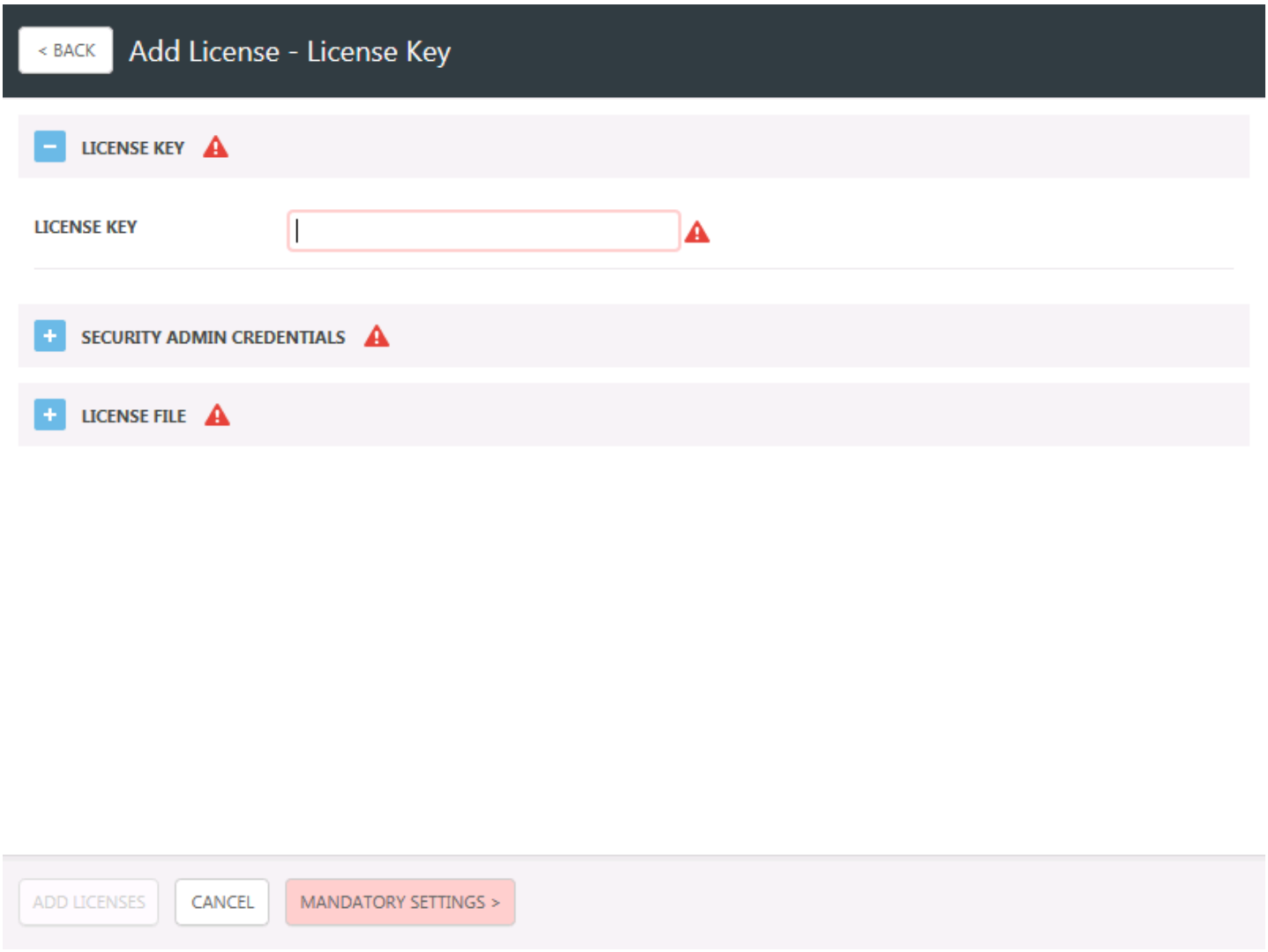
Select a license from the list above and click this option to remove it completely. You will be asked to confirm this action. Removal of the license does not trigger deactivation of the product. ESET product remains activated even when license has been deleted in ERA License Management.

6.1.9.1 Activation

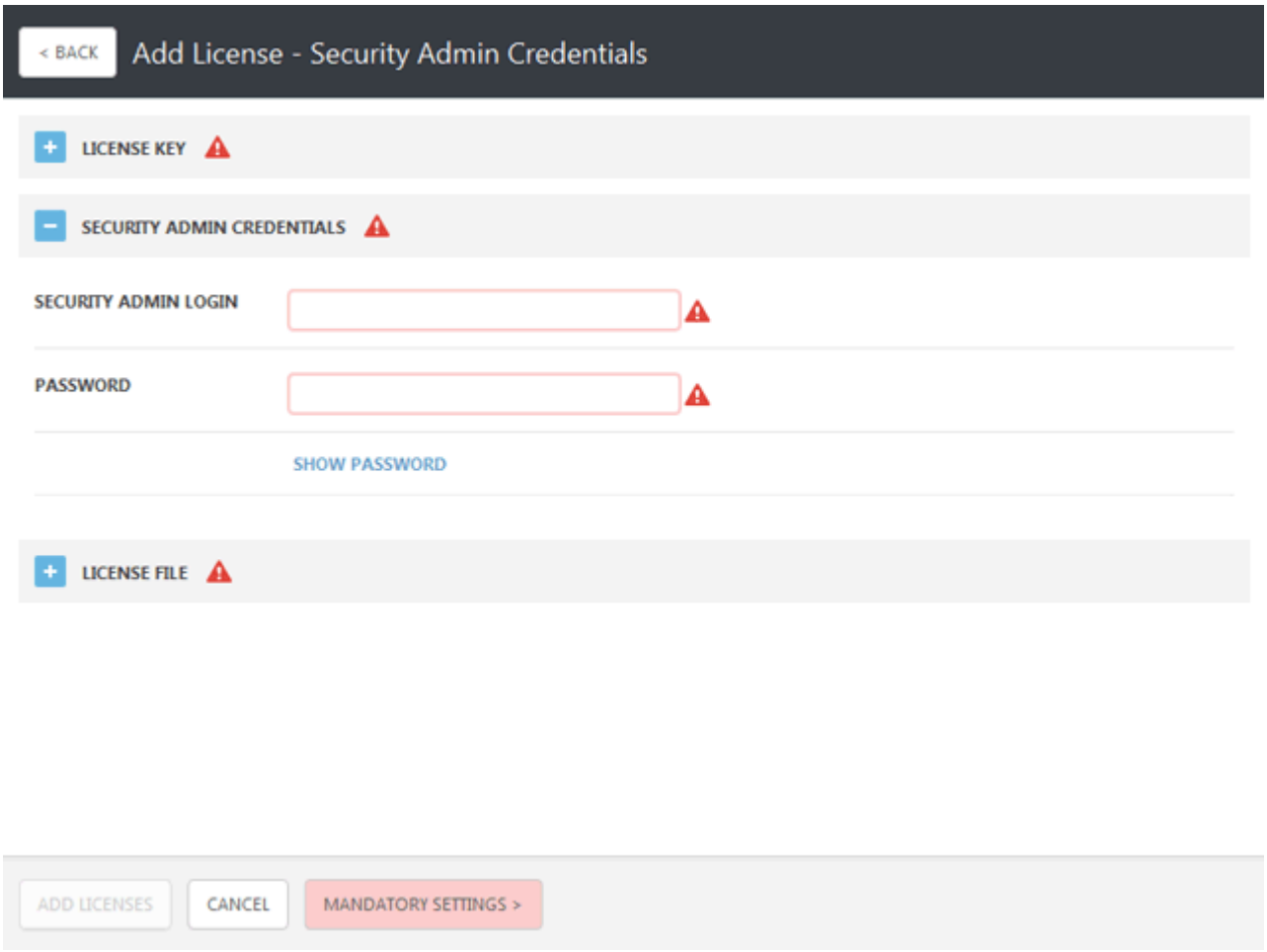
Navigate to **Admin** > **License Management** and click **Add Licenses**.



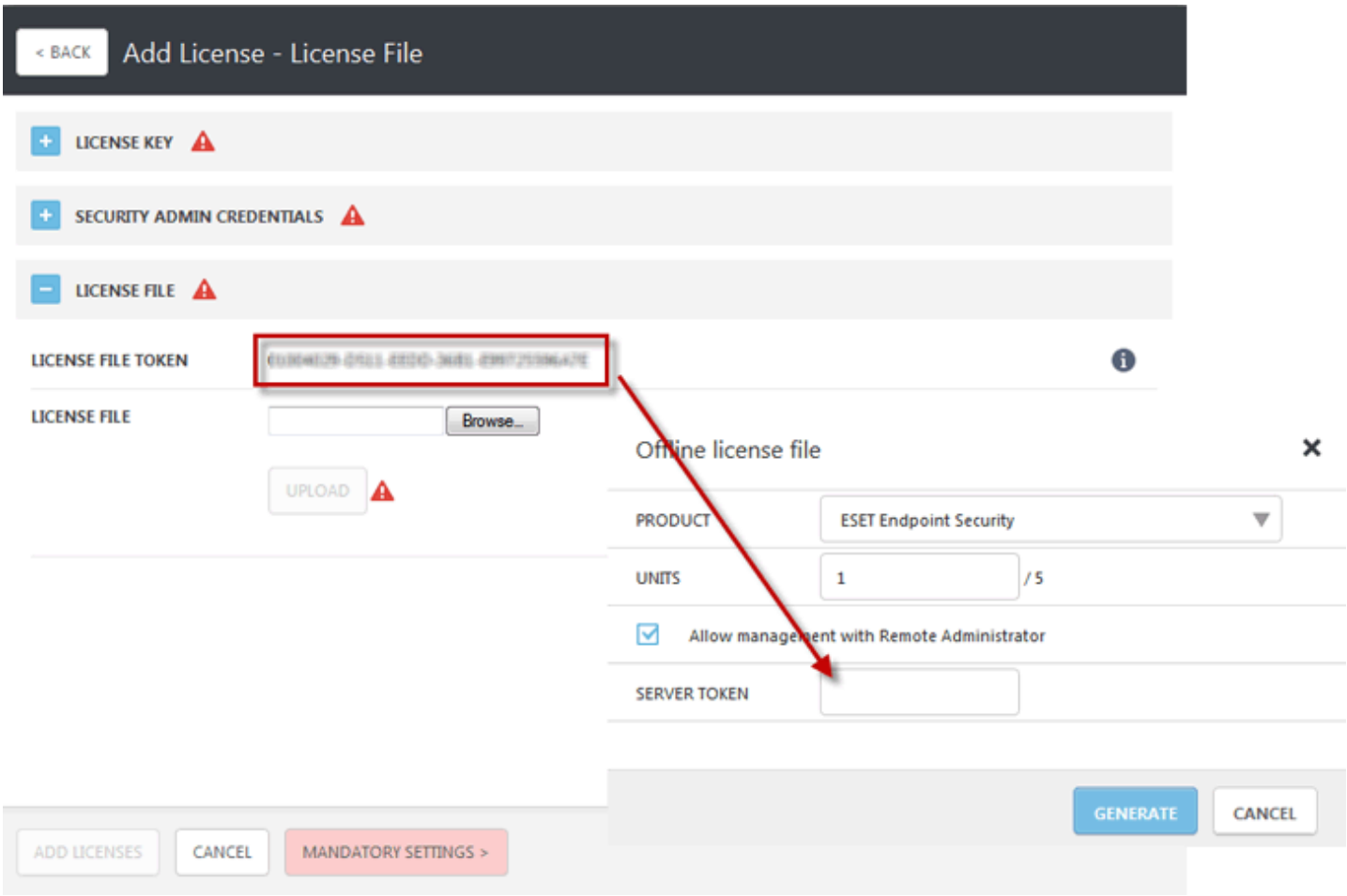
- Type or copy and paste the **License key** you received when you purchased your ESET security solution in to the **License Key** field. If you are using legacy license credentials (a Username and password), convert the credentials to a license key. If the license is not registered, it will trigger the registration process, which will be done on the ELA portal (ERA will provide the URL valid for registration based on the origin of the license).



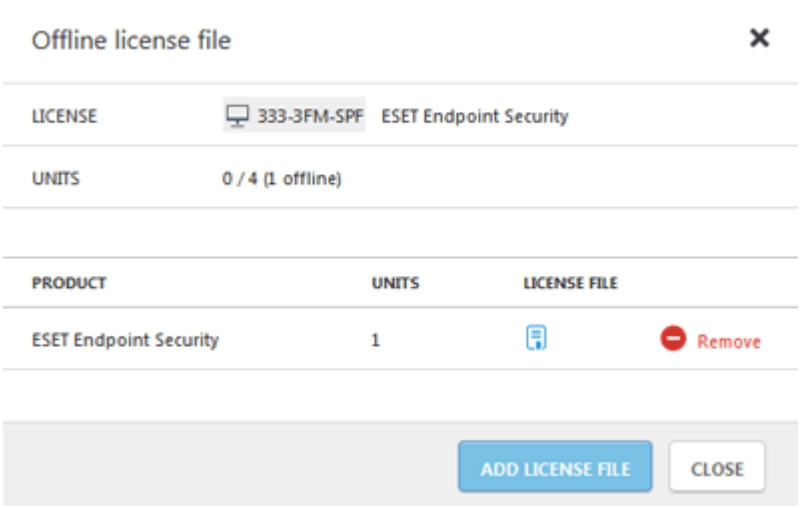
- Enter the **Security Admin** account credentials (ERA will display all delegate licenses later in ERA License Manager).



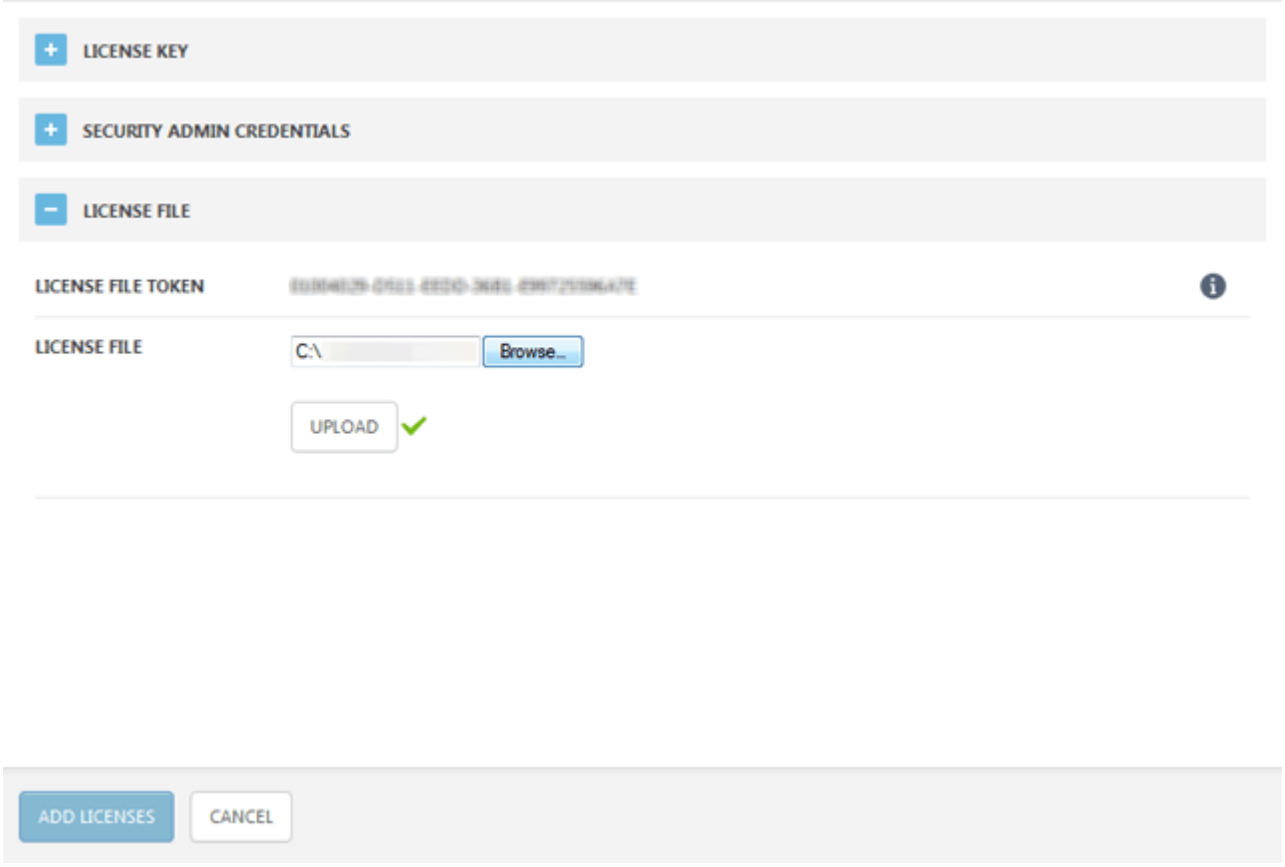
- Enter the **Offline license file** - you need to export using the ELA portal and include the information about product(s) ERA is able to manage. You will need to enter a specific **License file token** into ESET License Administrator portal when generating an offline license file, otherwise the license file won't be accepted by ESET Remote Administrator.



Click the document symbol to save the offline license file.



Go back to ERA License Management, click **Add licenses**, Browse for the offline license file you've exported in ELA and then click **Upload**.


LICENSE KEY
SECURITY ADMIN CREDENTIALS
LICENSE FILE
LICENSE FILE TOKEN
LICENSE FILE
C:\
Browse...
UPLOAD

ADD LICENSES
CANCEL

7. Diagnostic Tool

Diagnostic tool is a part of all ERA components. It is used to collect and pack logs that are used by developers to solve problems with product components. Run the Diagnostic tool, select a root folder where the logs will be saved, and then select the actions to be taken (see **Actions** below).

Location of the **Diagnostic Tool**:

Windows

Folder *C:\Program Files\ESET\RemoteAdministrator\<product>* , a file called **Diagnostic.exe**.

Linux

Path on the server: */opt/eset/RemoteAdministrator/<product>/* , there is a **Diagnostic<product>** executable (one word, for example, **DiagnosticServer**, **DiagnosticAgent**)

Actions

- **Dump logs** - A logs folder is created where all logs are saved.
- **Dump process** - A new folder is created. A process dump file is generally created in cases where a problem was detected. When a serious problem is detected, a dump file is created by system. To check it manually, go to the folder %temp% (in Windows) or folder /tmp/ (in Linux) and insert a dmp file.
  NOTE: Service (Agent, Proxy, Server, RD Sensor, FileServer) must be running.
- **General application information** - The GeneralApplicationInformation folder is created and inside it the file GeneralApplicationInformation.txt. This file contains text information including the product name and product version of the currently installed product.
- **Action configuration** - A configuration folder is created where file storage.lua is saved.

8. Glossary

8.1 Types of infiltration

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

8.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses mainly attack executable files and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its pre-defined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program by him/herself.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term "virus" is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term "malware" (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state – i.e., to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

8.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves – they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes of their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

8.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past– oday, there is no longer a need for them to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

- **Downloader** – A malicious program with the ability to download other infiltrations from the Internet
- **Dropper** – A type of trojan horse designed to drop other types of malware onto compromised computers
- **Backdoor** – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it
- **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers
- **Dialer** – Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

Examples of well-known trojans are: NetBus, Trojandownloader. Small.ZL, Slapper

8.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data, etc. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1) When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2) When they are hidden from the usual testing. ESET Remote Administrator users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

8.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry.If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

8.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

8.1.7 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET Remote Administrator provides the option to detect such threats.

"Potentially unsafe applications" is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

8.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

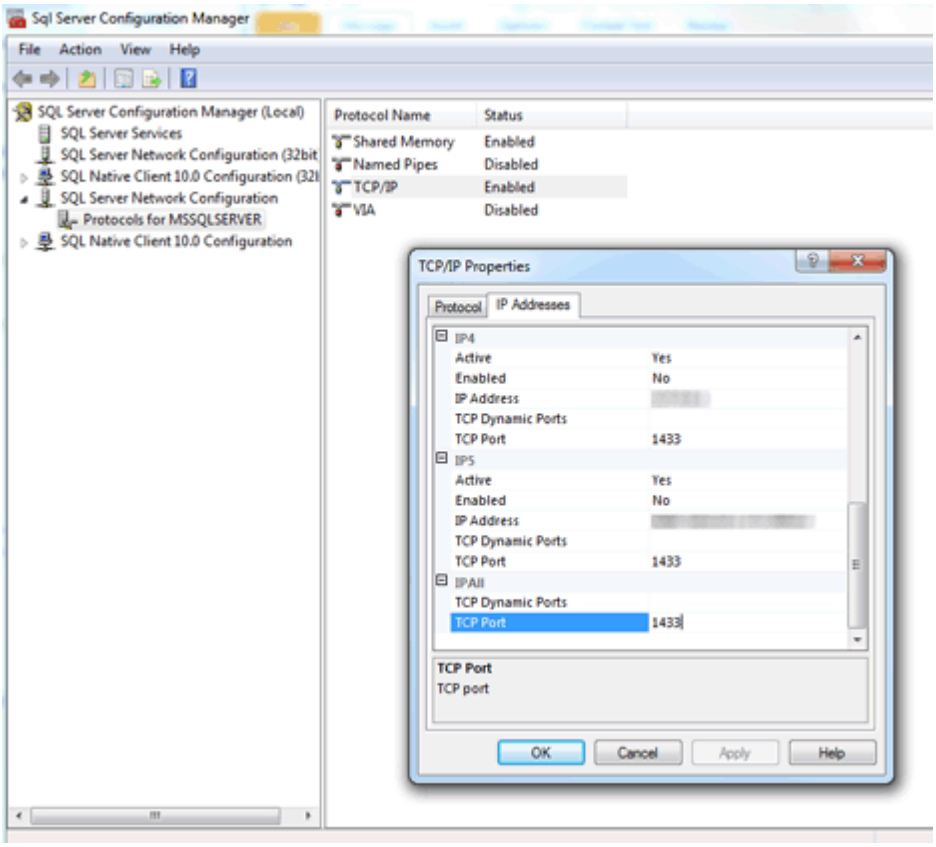
- New windows you haven't seen previously are opened
- Activation and running of hidden processes
- Increased usage of system resources
- Changes in search results
- Application communicates with remote servers

9. FAQ

Q: Why are we installing Java on a server? Doesn't this create a security risk?
A: ERA Web Console requires Java to function. Java is an industry standard for web-based consoles. Although ERA Web Console requires at least Java version 7, we strongly recommend that you use the latest officially released version of Java.

Q: The following error message is continuously logged in ESET Rogue Detector's trace.log: *2015-02-25 18:55:04 Information: CPCAPDeviceSniffer [Thread 764]: CPCAPDeviceSniffer on rpcap://\Device\NPF_{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error: Device open failed with error:Error opening adapter: The system cannot find the device specified. (20)*
A: This is a problem with WinPcap, stop the ESET Rogue Detector Sensor service, reinstall the latest version of WinPcap (at least 4.1.0) and restart the ESET Rogue Detector Sensor service.

Q: How do I determine which port is being used by SQL Server?
A: There are multiple ways to determine the port used by SQL Server. You can get the most accurate result via SQL Server Configuration Manager. See the figure below for an example of where to locate this information in SQL configuration manager:



Q: After installing SQL Express 2008 (included in ERA package) on Windows Server 2012 it doesn't appear to be listening on a standard SQL port.
A: It is most likely listening to a port other than the default, port 1433.

Q: How do I configure MySQL to accept large packet size?
A: Locate your MySQL configuration file (**my.ini** for Windows and **my.cnf** for Linux, the exact location of the .ini file might differ from one operating system to another), open this file and find the section `[mysqld]`. Add a new line `max_allowed_packet=33M` (value must be at least 33M or greater).

Q: If I install SQL myself, how should I create a database for ERA?
A: You don't have to. A database is created by the **Server.msi** installer, not by ERA Installer. The ERA Installer is included to simplify steps for you, it installs SQL Server and the database is created by the server.msi installer.

Q: Can ERA installer create a new database for me in an existing SQL Server installation, if I give it the proper SQL Server connection details and credentials? It would be convenient if the installer supported different versions of SQL Server (2008, 2014, etc.)
A: Database is created by **Server.msi**, so yes it can create an ERA database for you on individually installed SQL Server instances. And yes, the supported versions of SQL Server are 2008, 2012, 2014.

Q: Why is SQL version 2008 R2 used in ERA Installer?
A: SQL version 2008 R2 is used because Microsoft declares compatibility for this database type on Windows XP and later operating systems.

Q: What do I do when I get an **error code: -2068052081** during MSSQL installation?
A: Restart your computer and run setup again. If the issue persists, uninstall SQL Server Native Client and run installation again. If this does not resolve the issue, uninstall all Microsoft SQL Server products, restart your computer and then run installation again.

Q: What do I do when I get an **error code: -2067922943** during MSSQL installation?
A: Make sure your system meets the database requirements for ERA.

Q: If installing on an existing SQL Server, should the SQL Server use built-in Windows Authentication mode by default?
A: No, because Windows Authentication mode can be disabled on SQL Server and the only way to log in is to use SQL Server Authentication (entering a username and password). You need to use either SQL Server Authentication or Mixed Mode. When manually installing SQL Server, we recommend that you create a root password for SQL Server (root user is named “sa”, which stands for security admin) and store it for later in a safe place. The Root password may be needed when upgrading ERA Server.

Q: I had to install **Microsoft .NET Framework 3.5** as ERA Installer pointed me to (http://www.microsoft.com/en-us/download/details.aspx?id=21), but that didn't work on a fresh installation of Windows Server 2012 R2 with SP1.
A: This installer cannot be used on Windows Server 2012 because of the security policy on Windows Server 2012. Microsoft .NET Framework must be installed via the **Roles and Features Wizard**.

Q: Microsoft .NET 4.5 framework was already installed on my system. I had to use the Roles and Features Wizard to add .NET 3.5. Why doesn't ESET Remote Administrator support .NET 4.5?
A: Because .NET 4.5 is not backwards compatible with .NET 3.5, which is a prerequisite of SQL Server installer.

Q: It is very difficult to tell whether SQL Server installation is running. How can I tell what is happening if the installation takes more than 10 minutes?
A: SQL Server installation can, in rare cases, take up to 1 hour. Install times depend on system performance.

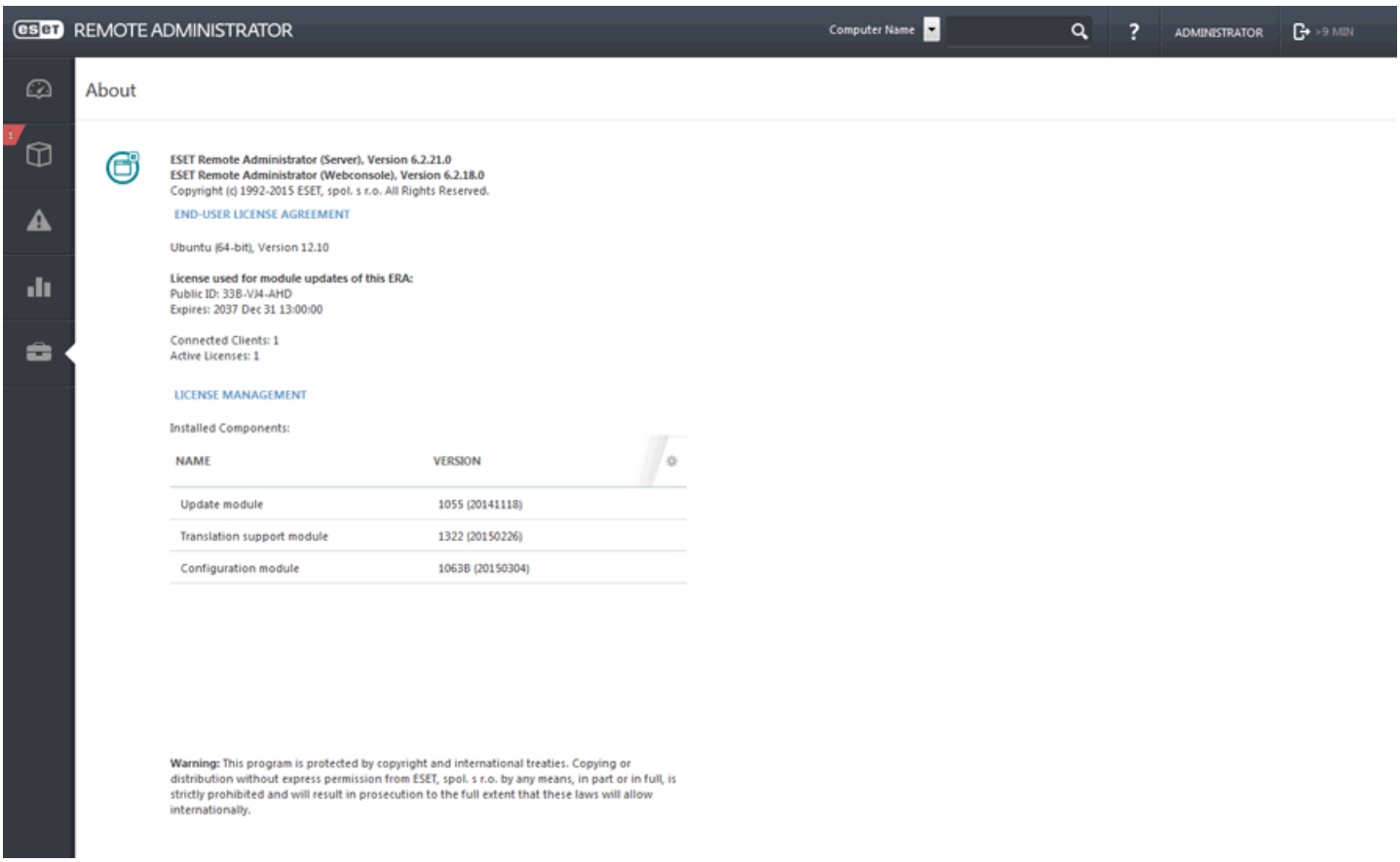
Q: How do I **reset the Administrator password** for Web Console (entered during set up)?
A: It is possible to reset the password by running the server installer and choosing **Repair**. Note that you may require the password for the ERA database if you did not use Windows Authentication during creation of the database.

NOTE: Please be careful, some of the repair options can potentially remove stored data.

Q: When importing a file containing a list of computers to add to ERA, what is the format required for the file?
A: File with following lines:
All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX
All is the required name of root group.

10. About ESET Remote Administrator

This window provides details about the installed version of ESET Remote Administrator and the list of installed program modules. The top part of the window contains information about your operating system and system resources.


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
About
ESET Remote Administrator (Server), Version 6.2.21.0
ESET Remote Administrator (Webconsole), Version 6.2.18.0
Copyright (c) 1992-2015 ESET, spol. s r.o. All Rights Reserved.
END-USER LICENSE AGREEMENT
Ubuntu (64-bit), Version 12.10
License used for module updates of this ERA:
Public ID: 33B-VJ4-AHD
Expires: 2037 Dec 31 13:00:00
Connected Clients: 1
Active Licenses: 1
LICENSE MANAGEMENT
Installed Components:
NAME
VERSION
Update module
1055 (20141118)
Translation support module
1322 (20150226)
Configuration module
1063B (20150304)
Warning: This program is protected by copyright and international treaties. Copying or distribution without express permission from ESET, spol. s r.o. by any means, in part or in full, is strictly prohibited and will result in prosecution to the full extent that these laws will allow internationally.

11. End-User License Agreement (EULA)

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS**.

Software End-User License Agreement.

Under the terms of this Software End User License Agreement (hereinafter referred to as “the Agreement”) executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31 333 535 or another company from the ESET Group (hereinafter referred to as "ESET" or “the Provider”) and you, a physical person or legal entity (hereinafter referred to as “You" or "the End User”), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END-USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on the "I Accept" option while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement. If You do not agree to all of the terms and conditions of this Agreement, immediately click on the "I Do Not Accept" option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to ESET or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) the computer program ESET Remote Administrator and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software (hereinafter referred to as “Documentation”); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the computer on which You install the Software.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement, You pay the License Fee within the maturity period and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("the License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses**. The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one computer system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as “an MUA”). If an MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (for example,, through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one computer.

c) **Business Edition**. A Business Edition version of the Software must be obtained to use the Software on mail servers, mail relays, mail gateways or Internet gateways.

d) **Term of the License**. Your right to use the Software shall be time-limited.

e) **OEM Software**. OEM Software shall be limited to the computer You obtained it with. It cannot be transferred to a different computer

f) **NFR, TRIAL Software**. Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License**. The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software.

4. **Connection to the Internet**. To operate correctly the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers. Connection to the Internet is necessary for the following features of the Software:

a) **Updates to the Software**. The Provider shall be entitled from time to issue updates to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled automatic installation of Updates.

b) **Forwarding of infiltrations and information to the Provider**. The Software contains a function which collects samples of new computer viruses, other similar harmful computer programs and suspicious or problematic files (hereinafter referred to as “Infiltrations”) and then sends them to the Provider, along with information about the computer and/or the platform on which the Software is installed (hereinafter referred to as “Information”). The Information may contain data (including personal data) about the End User and/or other users of the computer on which the Software is installed, information about the computer, the operating system and programs installed, files from the computer on which the Software is installed and files affected by an Infiltration and details about such files. The Provider shall only use Information and Infiltrations received for research into Infiltrations and shall take appropriate measures to ensure that the Information received remains confidential. By accepting this Agreement and activating the Software function described above, you are agreeing to Infiltrations and Information being sent to the Provider and you are also granting the Provider the necessary approval, as specified under the relevant legal regulations, for processing Information obtained.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those computer systems for which You have obtained a License.

6. **Restrictions to rights**. You may not copy, distribute, extract components or make derivative works of the Software. When using the Software You are required to comply with the following restrictions:

(a) You may make one copy of the Software on a permanent storage medium as an archival back-up copy, provided your archival back-up copy is not installed or used on any computer. Any other copies You make of the Software shall constitute breach of this Agreement.

(b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

(c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

(d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

(e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement**. This Agreement is effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own costs, the Software, all back-up copies and all related materials provided by the Provider or its business partners. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 20 and 22 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion.

16. **Transfer of the License**. The Software can be transferred from one computer system to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software**.The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent to the Provider containing licensing details (username and password) enabling Updates.

18. **Data regarding the End User and protection of rights**. As the End User, You hereby authorize the Provider to transfer, process and store data enabling the Provider to identify You. You hereby agree to the Provider using its own means to check whether You are using the Software in accordance with the provisions of this Agreement. You hereby issue your agreement to data being transferred, during communication between the Software and the Provider's computer systems or those of its business partners, the purpose of which is to ensure functionality of and authorization to use the Software and protection of the Provider’s rights. Following conclusion of this Agreement, the Provider or any of its business partners shall be entitled to transfer, process and store essential data identifying You, for billing purposes and performance of this Agreement. Details about privacy and personal data protection can be found on http://www.eset.com/privacy.

19. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities including the United States Government with the license rights and restrictions described in this Agreement.

20. **Export and re-export control**. The Software, the Documentation or components thereof, including information about the Software and components thereof, shall be subject to import and export controls under legal regulations which may be issued by governments responsible for issue thereof under applicable law, including US law. Export Administration Regulations and end-user, end-use and destination restrictions issued by the US Government and other governments. You agree to comply strictly with all applicable import and export regulations and acknowledge that You have the responsibility to obtain all licenses required to export, re-export, transfer or import the Software.

21. **Notices**. All notices and return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

22. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

23. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable in accordance with the conditions stipulated therein. This Agreement may only be modified in written form, signed by an authorized representative of the Provider or a person expressly authorized to act in this capacity under the terms of a power of attorney.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.